

30.11.2004

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: 2003年11月14日

出願番号
Application Number: 特願2003-385591
[ST. 10/C]: [JP2003-385591]

REC'D 23 DEC 2004

WIPO

PCT

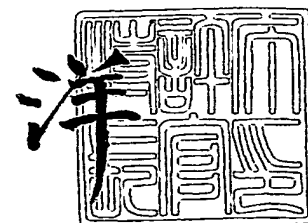
出願人
Applicant(s): ソニー株式会社
松下電器産業株式会社

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

2004年11月22日

特許庁長官
Commissioner,
Japan Patent Office

小川



【書類名】 特許願
【整理番号】 0390753704
【提出日】 平成15年11月14日
【あて先】 特許庁長官殿
【国際特許分類】 H04N 7/16
【発明者】
 【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社内
 【氏名】 北原 淳
【発明者】
 【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社内
 【氏名】 山下 雅美
【発明者】
 【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社内
 【氏名】 伊藤 哲規
【発明者】
 【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内
 【氏名】 山本 雅哉
【発明者】
 【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内
 【氏名】 小野田 仙一
【発明者】
 【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内
 【氏名】 村上 弘規
【特許出願人】
 【識別番号】 000002185
 【氏名又は名称】 ソニー株式会社
【特許出願人】
 【識別番号】 000005821
 【氏名又は名称】 松下電器産業株式会社
【代理人】
 【識別番号】 100082131
 【弁理士】
 【氏名又は名称】 稲本 義雄
 【電話番号】 03-3369-6479
【手数料の表示】
 【予納台帳番号】 032089
 【納付金額】 21,000円
【提出物件の目録】
 【物件名】 特許請求の範囲 1
 【物件名】 明細書 1
 【物件名】 図面 1
 【物件名】 要約書 1
 【包括委任状番号】 9708842

【書類名】 特許請求の範囲**【請求項 1】**

1 チャンネルの契約をすることで、その 1 チャンネルにより配信される複数のコンテンツが利用可能とされるコンテンツ配信サービスで用いられるライセンスを管理するライセンス管理方法において、

コンテンツの提供を受ける情報処理装置に対して、前記 1 チャンネルにより配信される複数のコンテンツ全体の利用条件を規定する第 1 のライセンスを提供し、

前記第 1 のライセンスとは別に、コンテンツ毎の利用条件を規定する第 2 のライセンスをコンテンツとともに前記情報処理装置に提供し、

前記第 1 のライセンスにより規定される利用条件と、前記第 2 のライセンスにより規定される利用条件のいずれも満たす場合、前記第 2 のライセンスとともに提供された前記コンテンツが前記情報処理装置において利用可能とされる

ことを特徴とするライセンス管理方法。

【請求項 2】

1 チャンネルの契約をすることで、その 1 チャンネルにより配信される複数のコンテンツが利用可能とされるコンテンツ配信サービスで提供されるコンテンツを処理する情報処理装置において、

前記 1 チャンネルにより配信される複数のコンテンツ全体の利用条件を規定する第 1 のライセンスを取得する第 1 の取得手段と、

前記第 1 のライセンスとは別に提供される、コンテンツ毎の利用条件を規定する第 2 のライセンスをコンテンツとともに取得する第 2 の取得手段と、

前記第 1 のライセンスにより規定される利用条件と、前記第 2 のライセンスにより規定される利用条件のいずれも満たす場合、前記第 2 のライセンスとともに提供された前記コンテンツの出力を制御する制御手段と

を備えることを特徴とする情報処理装置。

【請求項 3】

前記第 1 の取得手段は、用意される秘密鍵に対応する公開鍵により暗号化されて提供される前記第 1 のライセンスを取得する

ことを特徴とする請求項 2 に記載の情報処理装置。

【請求項 4】

前記制御手段は、前記第 1 のライセンスとともに提供される第 1 の鍵情報を用いて、前記第 2 のライセンスとともに暗号化されて提供される第 2 の鍵情報を復号し、復号して得られる前記第 2 の鍵情報により前記コンテンツに施されている暗号化を復号する

ことを特徴とする請求項 2 に記載の情報処理装置。

【請求項 5】

前記第 1 のライセンスにより規定される利用条件と、前記第 2 のライセンスにより規定される利用条件のいずれも満たす範囲内で、前記第 2 のライセンスとともに提供された前記コンテンツの利用を他の情報処理装置に許可するライセンス管理手段をさらに備える

ことを特徴とする請求項 2 に記載の情報処理装置。

【請求項 6】

複数のコンテンツが時間的に連続して前記 1 チャンネルにより配信される場合、

前記第 2 の取得手段は、第 1 のコンテンツに続けて配信される第 2 のコンテンツの利用条件を規定する前記第 2 のライセンスを前記第 1 のコンテンツの配信中に取得し、

前記制御手段は、前記第 1 のライセンスにより規定される利用条件と、前記第 2 の取得手段により取得された、前記第 2 のコンテンツの利用条件を規定する前記第 2 のライセンスにより規定される利用条件のいずれも満たす場合、前記第 1 のコンテンツに続けて出力されるように前記第 2 のコンテンツの出力を制御する

ことを特徴とする請求項 2 に記載の情報処理装置。

【請求項 7】

1 チャンネルの契約をすることで、その 1 チャンネルにより配信される複数のコンテンツが

利用可能とされるコンテンツ配信サービスで提供されるコンテンツを処理する情報処理方法において、

前記 1 チャンネルにより配信される複数のコンテンツ全体の利用条件を規定する第 1 のライセンスを取得する第 1 の取得ステップと、

前記第 1 のライセンスとは別に提供される、コンテンツ毎の利用条件を規定する第 2 のライセンスをコンテンツとともに取得する第 2 の取得ステップと、

前記第 1 のライセンスにより規定される利用条件と、前記第 2 のライセンスにより規定される利用条件のいずれも満たす場合、前記第 2 のライセンスとともに提供された前記コンテンツの出力を制御する制御ステップと

を含むことを特徴とする情報処理方法。

【請求項 8】

1 チャンネルの契約をすることで、その 1 チャンネルにより配信される複数のコンテンツが利用可能とされるコンテンツ配信サービスで提供されるコンテンツの処理をコンピュータに実行させるプログラムにおいて、

前記 1 チャンネルにより配信される複数のコンテンツ全体の利用条件を規定する第 1 のライセンスを取得する第 1 の取得ステップと、

前記第 1 のライセンスとは別に提供される、コンテンツ毎の利用条件を規定する第 2 のライセンスをコンテンツとともに取得する第 2 の取得ステップと、

前記第 1 のライセンスにより規定される利用条件と、前記第 2 のライセンスにより規定される利用条件のいずれも満たす場合、前記第 2 のライセンスとともに提供された前記コンテンツの出力を制御する制御ステップと

を含むことを特徴とするプログラム。

【書類名】 明細書**【発明の名称】** ライセンス管理方法、情報処理装置および方法、並びにプログラム**【技術分野】****【0001】**

本発明は、ライセンス管理方法、情報処理装置および方法、並びにプログラムに関し、特に、ユーザにとってはライセンスを容易に取得できるようにし、コンテンツの配信事業者にとってはコンテンツの著作権の保護を図りつつ、様々な形態のサービスに対応できるライセンスを提供することができるようにするライセンス管理方法、情報処理装置および方法、並びにプログラムに関する。

【背景技術】**【0002】**

近年、インフラストラクチャの整備に伴い、放送波を用いたもの、インターネットを用いたものなどの各種のコンテンツ配信サービスが実現されている。

【0003】

コンテンツ配信サービスにおいては、一般に、コンテンツの配信事業者と契約を行ったユーザのみがコンテンツを利用することができるように、或いは、ユーザによるコンテンツの正当な利用を確保し、コンテンツの著作権を保護することができるように、コンテンツを利用するにはコンテンツの利用条件を規定するライセンスが必要とされる。

【0004】

ライセンスの管理システムとしては、例えば、ユーザの自宅などに設置される受信機とライセンスを管理するサーバとの間で公開鍵暗号基盤に基づく通信を行い、インターネットを介してユーザにライセンスを提供するものや、CAS(Conditional Access System)によるものがある。

【0005】

公開鍵暗号基盤に基づく通信によりライセンスを管理するシステムによっては、例えば、コンテンツを利用する毎に所定のサーバにアクセスし、公開鍵証明書による認証を行うことが必要とされる。公開鍵証明書による認証が成立した場合にのみライセンスが提供されるため、このシステムによって、正当なユーザにのみライセンスが提供されるようにすることができ、コンテンツの著作権の保護を図ることができる。また、アクセスしてきたユーザの中から、CRL(Certificate Revocation List)と呼ばれるリストによって不正なユーザを排除することもできる。

【0006】

一方、CASによりライセンスを管理するシステムにおいては、配信されるコンテンツに、ユーザの自宅などに設置される受信機に挿入されるカードに記憶されている秘密鍵で解読可能となるように暗号化(スクランブル)が施されている。従って、ユーザは、コンテンツを利用する場合、映画チャンネル、スポーツチャンネル、音楽チャンネルのうちスポーツチャンネルのみを申し込むといった、チャンネル単位で契約を行い、秘密鍵の情報を配信事業者に登録する必要がある。登録した秘密鍵で解除できるようにスクランブルが施されるため、このシステムによっても、正当なユーザにのみコンテンツを利用させることができる。

【0007】

ところで、コンテンツ配信システムの構成等については特許文献1にも開示されている。

。 **【特許文献1】** 特開2003-69977号公報

【発明の開示】**【発明が解決しようとする課題】****【0008】**

しかしながら、公開鍵暗号基盤に基づく通信によりライセンスを管理するシステムにおいては、コンテンツを利用する毎に認証を行う必要があり、その分だけ時間や手間がかかるという課題があった。例えば、映画コンテンツを視聴したい場合でも、その視聴をすぐには開始させることができない。

【0009】

また、CASによりライセンスを管理するシステムにおいては、契約したチャネルで配信されるコンテンツが全て利用可能となるため、コンテンツを利用する毎に認証を行う必要はないものの、この場合、配信事業者からすれば、1つのチャネルで配信されるそれぞれのコンテンツに異なる利用条件を設定することが困難であるという課題があった。すなわち、コンテンツ毎に料金が発生したり、コンテンツ毎に異なる利用回数の制限を設定したりするなどの様々な形態のサービスに対応することが困難である。

【0010】

本発明はこのような状況に鑑みてなされたものであり、ユーザにとってはライセンスを容易に取得することができるようにするものである。また、コンテンツの配信事業者にとってはコンテンツの著作権の保護を図りつつ、様々な形態のサービスに対応できるライセンスを提供することができるようにするものである。

【課題を解決するための手段】

【0011】

本発明のライセンス管理方法は、1チャネルの契約をすることで、その1チャネルにより配信される複数のコンテンツが利用可能とされるコンテンツ配信サービスで用いられるライセンスを管理するライセンス管理方法であって、コンテンツの提供を受ける情報処理装置に対して、1チャネルにより配信される複数のコンテンツ全体の利用条件を規定する第1のライセンスを提供し、第1のライセンスとは別に、コンテンツ毎の利用条件を規定する第2のライセンスをコンテンツとともに情報処理装置に提供し、第1のライセンスにより規定される利用条件と、第2のライセンスにより規定される利用条件のいずれも満たす場合、第2のライセンスとともに提供されたコンテンツが情報処理装置において利用可能とされることを特徴とする。

【0012】

本発明の情報処理装置は、1チャネルの契約をすることで、その1チャネルにより配信される複数のコンテンツが利用可能とされるコンテンツ配信サービスで提供されるコンテンツを処理する情報処理装置であって、1チャネルにより配信される複数のコンテンツ全体の利用条件を規定する、第1のライセンスとは別に提供される、コンテンツ毎の利用条件を規定する第2のライセンスをコンテンツとともに取得する第2の取得手段と、第1のライセンスにより規定される利用条件と、第2のライセンスにより規定される利用条件のいずれも満たす場合、第2のライセンスとともに提供されたコンテンツの出力を制御する制御手段とを備えることを特徴とする。

【0013】

第1の取得手段は、用意される秘密鍵に対応する公開鍵により暗号化されて提供される第1のライセンスを取得するようにすることができる。

【0014】

制御手段は、第1のライセンスとともに提供される第1の鍵情報を用いて、第2のライセンスとともに暗号化されて提供される第2の鍵情報を復号し、復号して得られる第2の鍵情報によりコンテンツに施されている暗号化を復号するようにすることができる。

【0015】

本発明の情報処理装置は、第1のライセンスにより規定される利用条件と、第2のライセンスにより規定される利用条件のいずれも満たす範囲内で、第2のライセンスとともに提供されたコンテンツの利用を他の情報処理装置に許可するライセンス管理手段をさらに備えるようにすることができる。

【0016】

複数のコンテンツが時間的に連続して1チャネルにより配信される場合、第2の取得手段は、第1のコンテンツに続けて配信される第2のコンテンツの利用条件を規定する第2のライセンスを第1のコンテンツの配信中に取得し、制御手段は、第1のライセンスにより規定される利用条件と、第2の取得手段により取得された、第2のコンテンツの利用条件を規定する第2のライセンスにより規定される利用条件のいずれも満たす場合、第1の

コンテンツに続けて出力されるように第2のコンテンツの出力を制御するようにすることができる。

【0017】

本発明の情報処理方法は、1チャンネルの契約をすることで、その1チャンネルにより配信される複数のコンテンツが利用可能とされるコンテンツ配信サービスで提供されるコンテンツを処理する情報処理方法であって、1チャンネルにより配信される複数のコンテンツ全体の利用条件を規定する第1のライセンスを取得する第1の取得ステップと、第1のライセンスとは別に提供される、コンテンツ毎の利用条件を規定する第2のライセンスをコンテンツとともに取得する第2の取得ステップと、第1のライセンスにより規定される利用条件と、第2のライセンスにより規定される利用条件のいずれも満たす場合、第2のライセンスとともに提供されたコンテンツの出力を制御する制御ステップとを含むことを特徴とする。

【0018】

本発明のプログラムは、1チャンネルの契約をすることで、その1チャンネルにより配信される複数のコンテンツが利用可能とされるコンテンツ配信サービスで提供されるコンテンツの処理をコンピュータに実行させるプログラムであって、1チャンネルにより配信される複数のコンテンツ全体の利用条件を規定する第1のライセンスを取得する第1の取得ステップと、第1のライセンスとは別に提供される、コンテンツ毎の利用条件を規定する第2のライセンスをコンテンツとともに取得する第2の取得ステップと、第1のライセンスにより規定される利用条件と、第2のライセンスにより規定される利用条件のいずれも満たす場合、第2のライセンスとともに提供されたコンテンツの出力を制御する制御ステップとを含むことを特徴とする。

【0019】

本発明のライセンス管理方法においては、コンテンツの提供を受ける情報処理装置に対して、1チャンネルにより配信される複数のコンテンツ全体の利用条件を規定する第1のライセンスが提供され、第1のライセンスとは別に、コンテンツ毎の利用条件を規定する第2のライセンスがコンテンツとともに情報処理装置に提供され、第1のライセンスにより規定される利用条件と、第2のライセンスにより規定される利用条件のいずれも満たす場合、第2のライセンスとともに提供されたコンテンツが情報処理装置において利用可能とされる。

【0020】

本発明の情報処理装置および方法、並びにプログラムにおいては、1チャンネルにより配信される複数のコンテンツ全体の利用条件を規定する第1のライセンスが取得され、第1のライセンスとは別に提供される、コンテンツ毎の利用条件を規定する第2のライセンスがコンテンツとともに取得される。また、第1のライセンスにより規定される利用条件と、第2のライセンスにより規定される利用条件のいずれも満たす場合、第2のライセンスとともに提供されたコンテンツの出力が制御される。

【発明の効果】**【0021】**

本発明によれば、ユーザは、コンテンツの利用に必要なライセンスを容易に取得することができる。

【0022】

また、本発明によれば、コンテンツの配信事業者は、著作権の保護を図りつつ、コンテンツを配信することができる。

【0023】

さらに、本発明によれば、コンテンツの配信事業者は、様々な形態のサービスに対応することができるライセンスを提供することができる。

【発明を実施するための最良の形態】**【0024】**

以下に本発明の実施の形態を説明するが、本明細書に記載の発明と、発明の実施の形態

との対応関係を例示すると次のようになる。この記載は、請求項に記載されている発明をサポートする実施の形態が本明細書に記載されていることを確認するためのものである。従って、発明の実施の形態中には記載されているが、発明に対応するものとして、ここには記載されていない実施の形態があったとしても、そのことは、その実施の形態が、その発明に対応するものではないことを意味するものではない。逆に、実施の形態が発明に対応するものとしてここに記載されていたとしても、そのことは、その実施の形態が、その発明以外の発明には対応しないものであることを意味するものでもない。

【0025】

さらに、この記載は、本明細書に記載されている発明の全てを意味するものではない。換言すれば、この記載は、本明細書に記載されている発明であって、この出願では請求されていない発明の存在、すなわち、将来、分割出願されたり、補正により追加される発明の存在を否定するものではない。

【0026】

本発明によれば、ライセンス管理方法が提供される。このライセンス管理方法は、1チャンネルの契約をすることで、その1チャンネルにより配信される複数のコンテンツが利用可能とされるコンテンツ配信サービスで用いられるライセンスを管理するライセンス管理方法であって、コンテンツの提供を受ける情報処理装置（例えば、図1の受信機15-1乃至15-N）に対して、前記1チャンネルにより配信される複数のコンテンツ全体の利用条件を規定する第1のライセンス（例えば、メインライセンスの利用権利）を提供し、前記第1のライセンスとは別に、コンテンツ毎の利用条件を規定する第2のライセンス（例えば、サブライセンスの利用権利）をコンテンツとともに前記情報処理装置に提供し、前記第1のライセンスにより規定される利用条件と、前記第2のライセンスにより規定される利用条件のいずれも満たす場合、前記第2のライセンスとともに提供された前記コンテンツが前記情報処理装置において利用可能とされることを特徴とする。

【0027】

本発明によれば、情報処理装置が提供される。この情報処理装置（例えば、図1の受信機15-1乃至15-N）は、1チャンネルの契約をすることで、その1チャンネルにより配信される複数のコンテンツが利用可能とされるコンテンツ配信サービスで提供されるコンテンツを処理する情報処理装置であって、前記1チャンネルにより配信される複数のコンテンツ全体の利用条件を規定する第1のライセンス（例えば、メインライセンスの利用権利）を取得する第1の取得手段（例えば、図5のDRMコントローラ102）と、前記第1のライセンスとは別に提供される、コンテンツ毎の利用条件を規定する第2のライセンス（例えば、サブライセンスの利用権利）をコンテンツとともに取得する第2の取得手段（例えば、図5の受信機コントローラ101）と、前記第1のライセンスにより規定される利用条件と、前記第2のライセンスにより規定される利用条件のいずれも満たす場合、前記第2のライセンスとともに提供された前記コンテンツの出力を制御する制御手段（例えば、図5のコンテンツ復号部104）とを備えることを特徴とする。

【0028】

前記制御手段は、前記第1のライセンスとともに提供される第1の鍵情報（例えば、コンテンツ鍵Kc1）を用いて、前記第2のライセンスとともに暗号化されて提供される第2の鍵情報（例えば、コンテンツ鍵Kc2）を復号し、復号して得られる前記第2の鍵情報により前記コンテンツに施されている暗号化を復号するようにすることができる。

【0029】

本発明の情報処理装置は、前記第1のライセンスにより規定される利用条件と、前記第2のライセンスにより規定される利用条件のいずれも満たす範囲内で、前記第2のライセンスとともに提供された前記コンテンツの利用を他の情報処理装置（例えば、図14の情報処理端末121）に許可するライセンス管理手段（例えば、図14の「ライセンスA」を発行するDRMコントローラ102）をさらに備えるようにすることができる。

【0030】

複数のコンテンツが時間的に連続して前記1チャンネルにより配信される場合（図18に

示されるマルチキャストの場合)、前記第2の取得手段は、前記第1のコンテンツに続けて配信される第2のコンテンツの利用条件を規定する前記第2のライセンスを前記第1のコンテンツの配信中に取得し、前記制御手段は、前記第1のライセンスにより規定される利用条件と、前記第2の取得手段により取得された、前記第2のコンテンツの利用条件を規定する前記第2のライセンスにより規定される利用条件のいずれも満たす場合、前記第1のコンテンツに続けて出力されるように(シームレスに出力されるように)前記第2のコンテンツの出力を制御するようにすることができる。

【0031】

本発明によれば情報処理方法が提供される。この情報処理方法は、1チャンネルの契約をすることで、その1チャンネルにより配信される複数のコンテンツが利用可能とされるコンテンツ配信サービスで提供されるコンテンツを処理する情報処理方法であって、前記1チャンネルにより配信される複数のコンテンツ全体の利用条件を規定する第1のライセンス(例えば、メインライセンスの利用権利)を取得する第1の取得ステップ(例えば、図8のステップS42)と、前記第1のライセンスとは別に提供される、コンテンツ毎の利用条件を規定する第2のライセンス(例えば、サブライセンスの利用権利)をコンテンツとともに取得する第2の取得ステップ(例えば、図8のステップS34)と、前記第1のライセンスにより規定される利用条件と、前記第2のライセンスにより規定される利用条件のいずれも満たす場合、前記第2のライセンスとともに提供された前記コンテンツの出力を制御する制御ステップ(例えば、図9のステップS58)とを含むことを特徴とする。

【0032】

本発明によればプログラムが提供される。このプログラムにおいても、各ステップが対応する実施の形態(但し一例)は、本発明の情報処理方法と同様である。

【0033】

以下、本発明の実施の形態について図を参照して説明する。

【0034】

図1は、本発明を適用したコンテンツ配信システム1の構成例を示す図である。

【0035】

コンテンツ配信システム1は、インターネット11を介して相互に接続されるコンテンツサーバ12、ライセンスサーバ13、および、受信機15-1乃至15-Nから構成される。受信機15-1乃至15-Nのそれぞれを個々に区別する必要がある場合、適宜、まとめて受信機15と称する。

【0036】

コンテンツサーバ12は、例えば、コンテンツの制作会社により制作されたコンテンツを取得し、取得したコンテンツをインターネット11を介して受信機15(受信機15-1乃至15-N)に配信する。受信機15は、コンテンツサーバ12が配信するコンテンツを利用することについて、コンテンツ配信システム1を管理する配信事業者と契約するユーザの自宅などに設置されるものである。例えば、映画やドラマなどの動画コンテンツ、テキストや静止画像からなるニュース、天気予報などの静止画コンテンツ、音楽コンテンツなどがコンテンツサーバ12により配信される。

【0037】

コンテンツサーバ12により配信されるコンテンツには、そのコンテンツの利用条件を規定するライセンスが付加されている。コンテンツサーバ12は、ライセンスサーバ13により生成され、専用線14やインターネット11を介して供給されるライセンスを、それに対応するコンテンツとともに受信機15に配信する。以下、コンテンツの利用条件を規定し、コンテンツサーバ12からコンテンツとともに配信されるライセンスをサブライセンスと称する。

【0038】

ライセンスサーバ13は、サブライセンスをコンテンツサーバ12に提供するとともに、受信機15に対して、それぞれのユーザが契約するチャンネルで配信されるコンテンツ全体の利用条件を規定するライセンスを提供する。以下、1チャンネルで配信されるコンテン

ツ全体の利用条件を規定し、ライセンスサーバ13から受信機15のそれぞれに直接提供されるライセンスをメインライセンスと称する。

【0039】

なお、図1には、コンテンツサーバ12とライセンスサーバ13が1台ずつ示されているが、それぞれ複数設けられるようにしてもよい。また、コンテンツサーバ12の機能とライセンスサーバ13の機能をともに有する1台のサーバにより、コンテンツの配信とライセンスの生成が行われるようにしてもよい。

【0040】

ここで、サブライセンスとメインライセンスの関係について説明する。

【0041】

例えば、チャンネル単位で契約するいわゆるサブスクリプション(subscription)サービスでは、映画のみを配信するチャンネル、ドラマのみを配信するチャンネル、スポーツ番組のみを配信するチャンネルなどが用意されており、ユーザは、その中から1つのチャンネルの契約を行うことで、契約したチャンネルで配信される全てのコンテンツを視聴することができる。

【0042】

図2には、そのようなサブスクリプションサービスにおいて、コンテンツA乃至Xがチャンネル#1により配信されることが示されている。例えば、受信機15-1のユーザがチャンネル#1の契約を行った場合、コンテンツA乃至X全体の利用条件を規定する1つのメインライセンスが受信機15-1に提供される。

【0043】

また、コンテンツA乃至Xと、それぞれの利用条件を規定するサブライセンスA乃至Xが対応することが図2に示されており、ユーザにより選択されたコンテンツとともに、それに対応するサブライセンスが受信機15-1に提供される。サブライセンスには、対応するコンテンツの利用条件を規定する利用権利や、施されている暗号を復号する鍵情報などが含まれる。

【0044】

受信機15-1においては、例えば、コンテンツAを利用することがユーザにより指示されたとき、コンテンツサーバ12からコンテンツAとともに送信されてくるサブライセンスAと、ライセンスサーバ13から予め提供されているチャンネル#1のメインライセンスに基づいて、コンテンツAの再生が許可されているか否かの判定が行われ、許可されていると判定された場合にコンテンツAの再生が行われる。具体的には、メインライセンスで規定される利用条件を満たしており、かつ、サブライセンスAで規定される利用条件をも満たしている場合にのみコンテンツAの再生が行われる。

【0045】

このように、図1のコンテンツ配信システム1においては、1つのチャンネルで配信されるコンテンツ全体の利用条件を規定するメインライセンスと、そのチャンネルで配信されるコンテンツのそれぞれの利用条件を規定するサブライセンスとが異なる経路でユーザ（受信機15）に提供され、両方の利用条件を満たす場合にコンテンツが利用可能とされる。

【0046】

なお、メインライセンスは、例えば、ISO-9798-3で規定される非対称鍵暗号技術に基づく相互認証と鍵の交換による暗号鍵によって暗号化が施され、ライセンスサーバ13から受信機15に提供される。

【0047】

図1の説明に戻り、受信機15は、ユーザからの指示に応じて、コンテンツサーバ12からコンテンツとともに提供されるサブライセンスと、ライセンスサーバ13から提供されるメインライセンスに基づいてコンテンツを再生する。受信機15には、例えば、映像を出力するディスプレイ、音声を出力するスピーカなどが有線または無線により接続されており、それにより、受信機15により再生されたコンテンツが出力される。

【0048】

以上のように、コンテンツとともにサブライセンスが提供されるため、受信機15においては、コンテンツの再生が指示される毎に、コンテンツのライセンスを管理するサーバにアクセスして認証を行うなどの処理は行われず、すなわち、ライセンスを容易に取得することができ、ユーザがコンテンツの再生を指示してから、その出力が開始されるまでの時間を短縮させることができる。

【0049】

また、配信事業者としても、メインライセンスで規定するコンテンツ全体の利用条件だけでなく、サブライセンスによってそれぞれのコンテンツの利用条件を規定することができるため、様々な形態のコンテンツ配信サービスを提供することができる。例えば、メインライセンスでコンテンツ全体の利用期限を規定し、サブライセンスでそれぞれのコンテンツの視聴回数を規定するなど、1つのライセンスでは困難な、複雑な利用条件を規定し、サービスを提供することができる。

【0050】

例えば、コンテンツとともに配信されるライセンスのみで、そのコンテンツの利用期限と視聴回数を規定するようにすることもできるが、この場合、あるチャンネルで配信される全てのコンテンツに利用期限の情報も付加されることになり、全てのコンテンツに共通の利用期限の情報をメインライセンスによりまとめて規定する場合に較べてデータ量が多くなり、通信時間、処理時間が長くなる。また、後述するように、サブライセンスを利用するためには、メインライセンスに含まれる鍵情報が必要とされるため、2つのライセンスが1つの経路で提供される場合に較べてセキュリティを向上させることができる。

【0051】

図3A、Bは、メインライセンスとサブライセンスに含まれる情報の例を示す図である。

【0052】

図3Aに示されるように、メインライセンスには、ユーザが契約するチャンネル番号やチャンネルの名前（例えば、映画チャンネル）などを含み、そのチャンネルで配信されるコンテンツ全体の利用条件を規定する利用権利、サブライセンスの一部（利用権利、コンテンツ鍵Kc2、識別情報）の暗号化鍵であるコンテンツ鍵Kc1、メインライセンス作成者（例えば、ライセンスサーバ13の管理者）の電子署名、利用状況、利用実績が含まれる。

【0053】

電子署名が付加されることから、受信機15は、提供されたライセンスがどの装置により生成されたものであるのかを確認することができる。また、受信機15は、そのライセンスが正当なライセンスであるのか否かを確認することができる。

【0054】

利用状況と利用実績は、何も記録されていない状態で受信機15に提供され、ユーザがコンテンツを利用する毎に更新される。利用状況は、どのコンテンツが、どれくらい利用されたのかを表す。例えば、「10回利用できるコンテンツAを1回利用済みである」ことや、「10時間利用できるコンテンツAを1時間利用済みである」ことを表す情報が利用状況としてメインライセンスにより管理される。利用実績は、コンテンツの利用履歴を表す。この利用実績の内容は、必要に応じて受信機15からサーバ側（例えば、ライセンスサーバ13）に通知される。

【0055】

図3Bに示されるように、サブライセンスには、各コンテンツの利用条件を規定する利用権利、コンテンツの暗号化鍵であるコンテンツ鍵Kc2、このサブライセンスに対応するメインライセンスを識別するメインライセンスの識別情報、および、サブライセンス作成者（例えば、ライセンスサーバ13の管理者）の電子署名が含まれる。

【0056】

これらの情報のうちの利用権利、コンテンツ鍵Kc2、識別情報は、メインライセンスにより提供されるコンテンツ鍵Kc1により暗号化される。すなわち、受信機15においてコンテンツを再生するためには、サブライセンスに含まれるコンテンツ鍵Kc2が必要になり

、このコンテンツ鍵Kc2を取得するためにはメインライセンスに含まれるコンテンツ鍵Kc1が必要になる。

【0057】

また、識別情報は、図3Bに示されるように、コンテンツ鍵Kc1によって暗号化される情報の他、暗号化されない情報も用意される。識別情報を暗号化することにより、悪意者によりサブライセンスとメインライセンスの不正な対応付けが行われることを防止することができる。また、識別情報に暗号化が施されていない場合、サブライセンスを取得した受信機15は、識別情報を復号することなく、対応するメインライセンス（チャンネル）の検索等を行うことができる。

【0058】

このような各情報を含むメインライセンスとサブライセンスがそれぞれ異なる経路でユーザに提供される。

【0059】

図4は、図1のコンテンツサーバ12とライセンスサーバ13の機能構成例を示すブロック図である。

【0060】

コンテンツサーバ12のコンテンツ取得部61は、例えば、映画コンテンツ、ドラマコンテンツ、或いは音楽コンテンツなどの各種のコンテンツを、コンテンツサーバ12に装着された記録媒体やインターネット11を介して取得する。コンテンツ取得部61は、取得したコンテンツを暗号化部62に出力する。

【0061】

暗号化部62は、コンテンツ取得部61から供給されるコンテンツを、ライセンスサーバ13のコンテンツ鍵取得部81から専用線14やインターネット11を介して供給されるコンテンツ鍵Kc2を用いて暗号化し、得られたデータ（Enc（Kc2，コンテンツ））を配信データ生成部63に出力する。図4において、「Enc（Kc2，コンテンツ）」は、「コンテンツ」が「コンテンツ鍵Kc2」により暗号化されていることを表す。

【0062】

配信データ生成部63は、暗号化部62から供給されるデータ（Enc（Kc2，コンテンツ））に、ライセンスサーバ13のサブライセンス生成部85から供給されるサブライセンスを付加することで配信データを生成する。上述したように、このサブライセンスには、サブライセンスが付加されるコンテンツの利用条件を規定する利用権利が含まれている（図3）。配信データ生成部63により生成された配信データは配信データ記憶部64に記憶される。なお、図4において、枠で囲まれるコンテンツに付されている斜線は、コンテンツに暗号化が施されていることを表している。

【0063】

配信部65は、配信データ記憶部64に記憶されている配信データを受信機15からの要求に応じて読み出し、読み出した配信データをインターネット11を介して配信する。

【0064】

ライセンスサーバ13のコンテンツ鍵取得部81は、例えば、自ら生成するなどしてコンテンツ鍵Kc2を取得し、取得したコンテンツ鍵Kc2を暗号化部83と、コンテンツサーバ12の暗号化部62に出力する。

【0065】

情報取得部82は、例えば、コンテンツに設定する利用条件としてライセンスサーバ13の管理者により入力された情報に基づいて、サブライセンスに含める利用権利と、対応するメインライセンスの識別情報を取得する。情報取得部82は、取得した利用権利と識別情報を暗号化部83に出力する。

【0066】

暗号化部83は、コンテンツ鍵取得部81から供給されるコンテンツ鍵Kc2、情報取得部82から供給される利用権利、識別情報を、コンテンツ鍵取得部86から供給されるコンテンツ鍵Kc1を用いて暗号化し、得られたデータ（Enc（Kc1，（Kc2，利用権利、識

別情報))) を署名生成部 84 の出力と合成したものをサブライセンス生成部 85 に出力する。

【0067】

署名生成部 84 は、予め用意される秘密鍵を用いて電子署名を生成し、生成した電子署名と、暗号化部 83 から供給されてきたデータをサブライセンス生成部 85 に出力する。

【0068】

サブライセンス生成部 85 は、署名生成部 84 から供給されてきた電子署名を、暗号化部 83 により暗号化されたデータ (Enc (Kc1, (Kc2、利用権利、識別情報))) に付加し、図 3B に示されるサブライセンスを生成する。サブライセンス生成部 85 は、生成したサブライセンスを専用線 14 またはインターネット 11 を介してコンテンツサーバ 12 の配信データ生成部 63 に出力する。

【0069】

コンテンツ鍵取得部 86 はコンテンツ鍵 Kc1 を取得し、取得したコンテンツ鍵 Kc1 を暗号化部 83 とメインライセンス生成部 88 に出力する。

【0070】

情報取得部 87 は、例えば、ライセンスサーバ 13 の管理者により入力された情報に基づいてメインライセンスに含める利用権利を取得するとともに、ユーザによるコンテンツの利用状況、利用実績を管理する情報を取得する。例えば、ユーザがサブスクリプションサービスに加入し、複数用意されているチャンネルのうちの映画チャンネルの視聴を契約した場合、その映画チャンネルの視聴を許可する利用権利が情報取得部 87 により取得される。情報取得部 87 により取得された利用権利、利用状況、利用実績の各情報はメインライセンス生成部 88 に出力される。

【0071】

メインライセンス生成部 88 は、コンテンツ鍵取得部 86 から供給されるコンテンツ鍵 Kc1 と、情報取得部 87 から供給される利用権利、利用状況、利用実績の各情報に基づいて図 3A に示されるメインライセンスを生成する。生成されたメインライセンスはメインライセンス提供部 89 に出力される。

【0072】

メインライセンス提供部 89 は、メインライセンス生成部 88 により生成されたメインライセンスを、そのメインライセンスを利用してコンテンツを利用することについて契約を行っているユーザの受信機 15 に提供する。例えば、メインライセンス提供部 89 は、ISO-9798-3 で規定される非対称鍵暗号技術に基づく相互認証と鍵の交換による暗号鍵によってメインライセンスを暗号化し、受信機 15 に提供する。

【0073】

図 5 は、受信機 15 の機能構成例を示すブロック図である。

【0074】

受信機コントローラ 101 は、例えば、あるコンテンツの再生がユーザから指示されたとき、コンテンツサーバ 12 に対してコンテンツの送信を要求し、要求に応じて配信されてきた配信データを受信する。受信機コントローラ 101 は、配信データに含まれるコンテンツを暗号化コンテンツ記憶部 103 に出力し、サブライセンスを DRM (Digital Rights Management) コントローラ 102 に出力する。なお、暗号化コンテンツ記憶部 103 に出力されるコンテンツは、コンテンツ鍵 Kc2 で暗号化が施された状態のものであり、DRM コントローラ 102 に出力されるサブライセンスはその一部がコンテンツ鍵 Kc1 で暗号化が施された状態のものである。

【0075】

なお、受信機コントローラ 101 による配信データ (コンテンツ) のダウンロードは、チャンネルの契約が終了し、その代金の支払いが終了する前後などの所定のタイミングで自動的に開始されるようにしてもよい。また、ユーザの嗜好に合わせてコンテンツサーバ 12 が自発的にコンテンツを提供する、いわゆるプッシュ型のサービスである場合、受信機コントローラ 101 は、そのプッシュ型で提供される配信データを取得する。

【0076】

DRMコントローラ102は、例えば、ISO-9798-3で規定される非対称鍵暗号技術に基づく相互認証と鍵の交換による暗号鍵を用いて、暗号化が施された状態でライセンスサーバ3から送信されてくるメインライセンスを復号し、取得する。メインライセンスを取得する処理は、例えば、それぞれのチャンネル毎に1回ずつ行われる。

【0077】

また、DRMコントローラ102は、メインライセンスに含まれる電子署名の正当性の検証等を行った後、メインライセンスに含まれる利用権利、利用状況、利用実績を記憶部107に、コンテンツ鍵Kc1をコンテンツ鍵記憶部108にそれぞれ記憶させる。記憶部107に記憶された利用状況、利用実績は、再生部105によりコンテンツが再生される毎に更新される。

【0078】

さらに、DRMコントローラ102は、コンテンツの再生が指示されたとき、受信機コントローラ101から受信したサブライセンスをサブライセンス復号部106に送信する。受信機コントローラ101とDRMコントローラ102の処理についてはフローチャートを参照して後に詳述する。

【0079】

コンテンツ復号部104は、暗号化された状態のコンテンツを暗号化コンテンツ記憶部103から読み出し、読み出したコンテンツを、サブライセンス復号部106から供給されるコンテンツ鍵Kc2を用いて復号する。コンテンツ鍵Kc2は、メインライセンスとサブライセンスにより規定される利用条件から、コンテンツの再生が許可されていることが確認された場合にサブライセンス復号部106から供給される。コンテンツ復号部104により復号されたコンテンツは再生部105に出力される。

【0080】

再生部105は、コンテンツ復号部104により復号されたコンテンツに対してデコードやデジタルアナログ変換等の処理を施し、画像をディスプレイに、音声をスピーカ（いずれも図示せず）に出力する。

【0081】

サブライセンス復号部106は、DRMコントローラ102から供給されるサブライセンスの一部を、コンテンツ鍵記憶部108に記憶されているコンテンツ鍵Kc1を用いて復号する。サブライセンス復号部106は、サブライセンスに含まれる利用権利を利用条件確認部109に、コンテンツ鍵Kc2をコンテンツ復号部104にそれぞれ出力する。

【0082】

利用条件確認部109は、コンテンツの再生が許可されているか否かを確認することがDRMコントローラ102から指示されることに応じて、メインライセンスの利用権利を記憶部107から読み出す。また、利用条件確認部109は、サブライセンス復号部106により復号されたサブライセンスの利用権利を取得し、取得したサブライセンスの利用権利と、メインライセンスの利用権利に基づいて、コンテンツを利用することが許可されているか否かを確認する。利用条件確認部109は、コンテンツを利用することが許可されているか否かをDRMコントローラ102に通知する。

【0083】

署名検証部110は、DRMコントローラ102から受信したメインライセンスとサブライセンスの署名の検証を行う。サブライセンスはサブライセンス復号部106にてコンテンツ鍵Kc1を用いて復号され、サブライセンス内の利用権利、識別情報、コンテンツ鍵Kc2が取り出される。復号された情報と、これらの情報を元に計算された署名がDRMコントローラ102から署名検証部110に送られる。署名検証部110は署名の検証を行い、検証結果をDRMコントローラ102に知らせる。

【0084】

次に、以上のような構成を有するコンテンツサーバ12、ライセンスサーバ13、受信機15の動作についてフローチャートを参照して説明する。

【0085】

始めに、図6のフローチャートを参照して、メインライセンスとサブライセンスを生成するライセンスサーバ13のライセンス生成処理について説明する。

【0086】

ステップS1において、コンテンツ鍵取得部81はコンテンツ鍵Kc2を取得し、情報取得部82はサブライセンスの利用権利と、生成するサブライセンスが対応するメインライセンスの識別情報を取得する。サブライセンスの利用権利は、例えば、ライセンスサーバ13の管理者により入力された情報に基づいて情報取得部82により取得される。コンテンツ鍵Kc2はコンテンツ鍵取得部81から暗号化部83に出力され、利用権利、識別情報は情報取得部82から暗号化部83に出力される。

【0087】

ステップS2において、コンテンツ鍵取得部86はコンテンツ鍵Kc1を取得し、情報取得部87はメインライセンスに含める利用権利、ユーザによるコンテンツの利用状況、利用実績を管理する情報を取得する。メインライセンスに含まれる利用権利は、サブライセンスに含まれる利用権利と同様に、例えば、ユーザとの契約に応じてライセンスサーバ13の管理者により入力された情報から取得される。コンテンツ鍵Kc1はコンテンツ鍵取得部86から暗号化部83とメインライセンス生成部88に出力され、利用権利、利用状況、利用実績は情報取得部87からメインライセンス生成部88に出力される。

【0088】

メインライセンス生成部88は、ステップS3において、コンテンツ鍵取得部86から供給されるコンテンツ鍵Kc1と、情報取得部87から供給される利用権利、利用状況、利用実績の各情報に基づいてメインライセンスを生成する。なお、メインライセンスには、メインライセンス生成部88により生成された電子署名も含まれる。生成されたメインライセンスはメインライセンス提供部89に出力され、所定のタイミングで受信機15に提供される。

【0089】

ステップS4において、署名生成部84は、秘密鍵を用いてコンテンツ鍵取得部81と、情報取得部82から供給される、コンテンツ鍵Kc2、利用権利、識別情報の電子署名を生成する。

【0090】

ステップS5において、暗号化部83は、コンテンツ鍵取得部81から供給されるコンテンツ鍵Kc2、情報取得部82から供給される利用権利、識別情報を、コンテンツ鍵取得部86から供給されるコンテンツ鍵Kc1を用いて暗号化する。暗号化して得られたデータ(Enc(Kc1, (Kc2、利用権利、識別情報)))は、ステップS4の処理によって得られた電子署名と合わせてサブライセンス生成部85に出力される。

【0091】

ステップS6において、サブライセンス生成部85は、署名生成部84から供給された電子署名を、暗号化部83により暗号化されたデータ(Enc(Kc1, (Kc2、利用権利、識別情報)))に付加し、サブライセンスを生成する。

【0092】

ステップS7において、コンテンツ鍵取得部81は、コンテンツ鍵Kc2を専用線14またはインターネット11を介してコンテンツサーバ12の暗号化部62に送信する。また、サブライセンス生成部85は、サブライセンスを専用線14またはインターネット11を介してコンテンツサーバ12の配信データ生成部63に送信する。

【0093】

以上の処理により、ユーザが契約するチャンネルで配信されるコンテンツ全体の利用条件を規定するメインライセンス、および、それぞれのコンテンツの利用条件を規定するサブライセンスがライセンスサーバ13により生成される。

【0094】

次に、図7のフローチャートを参照して、コンテンツサーバ12の配信データ生成処理

について説明する。

【0095】

ステップS21において、コンテンツ取得部61はコンテンツを取得し、取得したコンテンツを暗号化部62に出力する。例えば、コンテンツサーバ12に装着された記録媒体に記録されているコンテンツ、或いは、インターネット11を介して送信されてきたコンテンツがコンテンツ取得部61により取得される。

【0096】

暗号化部62は、ステップS22において、コンテンツ取得部61から供給されるコンテンツを、ライセンスサーバ13のコンテンツ鍵取得部81から供給されるコンテンツ鍵Kc2を用いて暗号化する。暗号化を施すことで得られたデータ(Enc(Kc2, コンテンツ))は配信データ生成部63に出力される。

【0097】

ステップS23において、配信データ生成部63は、暗号化部62から供給されるデータ(Enc(Kc2, コンテンツ))に、ライセンスサーバ13のコンテンツ鍵取得部86から供給されるサブライセンスを付加することで配信データを生成する。

【0098】

配信データ生成部63により生成された配信データは配信データ記憶部64に出力され、ステップS24において記憶される。

【0099】

以上の処理により生成された配信データは、ユーザ(受信機15)からの要求に応じて配信可能な状態で配信データ記憶部64に記憶される。

【0100】

次に、図8および図9のフローチャートを参照して、受信機15においてコンテンツを再生する場合に、コンテンツサーバ12、ライセンスサーバ13、および受信機15の間で行われる処理について説明する。

【0101】

契約するチャンネルで配信されるコンテンツを取得することがユーザから指示されたとき、ステップS31において、受信機15の受信機コントローラ101は、インターネット11を介してコンテンツサーバ12にアクセスし、コンテンツの取得(配信データのダウンロード)を要求する。

【0102】

ステップS32において、コンテンツサーバ12の配信部65は、受信機15からの要求を受信し、ステップS33に進む。ステップS33において、配信部65は、要求されたコンテンツを含む配信データを配信データ記憶部64から読み出し、コンテンツ取得応答として、それを受信機15に送信する。

【0103】

受信機15の受信機コントローラ101は、ステップS34においてコンテンツサーバ12から送信されてきた配信データを受信し、ステップS35に進み、配信データに含まれるコンテンツを暗号化コンテンツ記憶部103に記憶させる。ステップS36において暗号化コンテンツ記憶部103に記憶されるコンテンツは、コンテンツ鍵Kc2で暗号化された状態のものである。

【0104】

受信機コントローラ101は、ステップS37においてDRMコントローラ102にメインライセンスの取得を要求する。なお、この要求は、ユーザが契約するチャンネルのメインライセンスが受信機15に取得されていない場合にのみ行われ、既に取得されている場合(記憶部107にメインライセンスの利用権利等が記憶され、コンテンツ鍵記憶部108にコンテンツ鍵Kc1が記憶されている場合)には行われない。

【0105】

DRMコントローラ102は、ステップS38において、受信機コントローラ101からの要求を受信し、ステップS39に進む。ステップS39において、DRMコントローラ1

02は、インターネット11を介してライセンスサーバ13にアクセスし、メインライセンスの取得（提供）を要求する。

【0106】

ライセンスサーバ13のメインライセンス提供部89は、ステップS40において、DRMコントローラ102からの要求を受信し、ステップS41に進む。このとき、図6を参照して説明した処理がライセンスサーバ13の各部により行われ、メインライセンスが生成される。

【0107】

ステップS41において、メインライセンス提供部89は、受信機15のユーザが契約するチャンネルのメインライセンスを、例えば、ISO-9798-3で規定される非対称鍵暗号技術に基づく相互認証と鍵の交換による暗号鍵を用いて暗号化し、ライセンス取得応答としてインターネット11を介して送信する。これにより、メインライセンスが第三者に漏洩したり、改竄されたりすることを防止することができる。

【0108】

DRMコントローラ102は、ステップS42において、ライセンスサーバ13から送信されてきたメインライセンスを受信する。DRMコントローラ102は、メインライセンスを受信したとき、メインライセンスに含まれる利用権利等の情報を記憶部107に記憶させ、コンテンツ鍵Kc1をコンテンツ鍵記憶部108に記憶させる。

【0109】

DRMコントローラ102は、ステップS43において、メインライセンスを取得したことをライセンス取得応答として受信機コントローラ101に通知する。

【0110】

取得したコンテンツの再生がユーザにより指示されたとき、受信機コントローラ101は、ステップS45において、DRMコントローラ102にコンテンツの再生を準備することを要求する。

【0111】

その要求をステップS46において受信したDRMコントローラ102は、ステップS47に進み、再生が指示されたコンテンツの利用条件を規定するサブライセンスをサブライセンス復号部106に出力し、その復号を要求する。

【0112】

サブライセンス復号部106は、ステップS48において、DRMコントローラ102からの要求を受信し、コンテンツ鍵記憶部108に記憶されているコンテンツ鍵Kc1を用いてサブライセンスを復号する。サブライセンスの復号が終了したとき、サブライセンス復号部106は、ステップS49に進み、復号が終了したことをサブライセンス復号応答としてDRMコントローラ102に通知する。サブライセンス復号部106により復号された利用権利（再生が指示されたコンテンツに対応するサブライセンスの利用権利）は利用条件確認部109に出力される。また、サブライセンスに含まれるコンテンツ鍵Kc2はコンテンツ復号部104に出力される。

【0113】

ステップS50において、DRMコントローラ102は、サブライセンス復号部106からの応答を受信し、ステップS51に進み、利用条件確認部109に利用条件の確認を要求する。

【0114】

利用条件の確認の要求をステップS52において受信した利用条件確認部109は、記憶部107に記憶されているメインライセンスの利用権利を読み出し、読み出したメインライセンスの利用権利と、サブライセンス復号部106から供給されるサブライセンスの利用権利の内容を確認する。利用条件確認部109は、メインライセンスの利用権利とサブライセンスの利用権利に基づいて、利用条件を満たすことを確認した場合、ステップS53において、コンテンツの再生が許可されていることを確認応答としてDRMコントローラ102に通知し、利用条件を満たさない場合、コンテンツの再生が許可されていないこ

とをDRMコントローラ102に通知する。

【0115】

ここで、利用条件確認部109が確認する利用条件について説明する。

【0116】

図10は、利用権利（利用条件）の具体例を示す図である。

【0117】

図10の例においては、コンテンツAを配信するチャネルの利用条件として、有効期限が2003年10月1日（2003/10/01）から2003年10月31日（2003/10/31）までであることがメインライセンスにより規定されている。また、コンテンツAの利用条件として10回利用可能であることがサブライセンスにより規定されている。

【0118】

従って、この場合、利用条件確認部109はコンテンツAの再生が指示された日時が2003年10月1日から2003年10月31日までの期間内であって、かつ、コンテンツAを既に10回利用したか否かを確認する。コンテンツAの再生が指示された日時が2003年10月1日から2003年10月31日までの期間内であって、かつ、コンテンツAをまだ10回利用していない場合、コンテンツAは利用可能であると判定される。また、コンテンツAの再生が指示された日時が2003年10月1日から2003年10月31日までの期間内ではない場合、または、コンテンツAを既に10回利用している場合、コンテンツAは利用不可能であると判定される。

【0119】

コンテンツAの利用回数等は、記憶部107に記憶されている利用状況、利用実績が参照される。

【0120】

また、図10の例においては、コンテンツBを配信するチャネルの利用条件として有効期限が2003年12月31日（2003/12/31）までであることがメインライセンスにより規定されている。また、コンテンツBの利用条件は規定されておらず、メインライセンスで規定される利用条件の範囲内であれば、コンテンツBは自由に利用することができるものとされている。従って、この場合、利用条件確認部109は、コンテンツBの再生が指示された日時が2003年12月31日までの期間内であるか否かを確認する。ここで確認する際に参照される時刻は、第三者に不正な改ざん等がされる恐れのない安全な経路で、時刻を管理するサーバから取得され、例えば、DRMコントローラ102の内部等のセキュアなモジュールにて管理される正確な時刻とされる。

【0121】

このように、メインライセンスとサブライセンスを用いることで、1チャネルで配信されるコンテンツ全体の利用条件と、それぞれのコンテンツの利用条件を規定することができる。従って、チャネル単位で契約するサブスクリプションサービスの場合であっても、その1チャネルで配信されるそれぞれのコンテンツに、利用期間や利用回数などの異なる条件を設定することができる。

【0122】

図9の説明に戻り、利用条件確認部109からの応答をステップS54において受信したDRMコントローラ102は、その応答に含まれる確認結果に基づいて、コンテンツの再生が許可されていると判定した場合、ステップS55に進み、コンテンツの再生準備応答として、コンテンツの再生を開始することを受信機コントローラ101に通知する。

【0123】

DRMコントローラ102からの通知をステップS56において受信した受信機コントローラ101は、ステップS57に進み、コンテンツ復号部104にコンテンツの復号を要求する。

【0124】

コンテンツ復号部104は、受信機コントローラ101からの要求をステップS58において受信し、サブライセンス復号部106から供給されるコンテンツ鍵Kc2を用いて、

復号が指示されたコンテンツ（暗号化コンテンツ記憶部103に記憶されている、暗号化された状態のコンテンツ）を復号する。

【0125】

コンテンツ復号部104により復号されたコンテンツは再生部105に出力され、ディスプレイやスピーカからコンテンツの内容が出力される。再生部105は、コンテンツを出力することに応じて、記憶部107に記憶されている利用状況、利用実績を更新させる。

。

【0126】

再生部105によるコンテンツの再生が終了したとき、コンテンツ復号部104は、ステップS59において、コンテンツの復号（再生）が終了したことをコンテンツ復号応答として受信機コントローラ101に通知する。

【0127】

以上の処理がコンテンツサーバ12、ライセンスサーバ13、および受信機15により実行され、ユーザにコンテンツが提供される。

【0128】

次に、図11のフローチャートを参照して、メインライセンスをライセンスサーバ13から取得するDRMコントローラ102のライセンス取得処理について説明する。

【0129】

ステップS71において、DRMコントローラ102は、ライセンスサーバ13からメインライセンスを取得することを要求する、ライセンス取得要求が受信機コントローラ101から送信されてきたか否かを判定し、送信されてきたと判定するまで待機する。図8を参照して説明したように、暗号化コンテンツ記憶部103にコンテンツが記憶された後、受信機コントローラ101からライセンス取得要求が送信されてくる（図8のステップS37）。

【0130】

ステップS71において、ライセンス取得要求が送信されてきたと判定した場合、DRMコントローラ102は、ステップS72に進み、例えば、それぞれのチャンネルのメインライセンスの取得状態を表すフラグ、或いは、記憶部107やコンテンツ鍵記憶部108に記憶されている情報を参照し、要求されたメインライセンスを取得済みであるか否かを判定する。

【0131】

ステップS72において、メインライセンスを取得済みであると判定した場合、DRMコントローラ102はステップS73に進み、受信機コントローラ101から要求されたチャンネルのメインライセンスを取得済みとしてフラグに設定し、後述するステップS74、S75の処理をスキップする。

【0132】

一方、ステップS72において、メインライセンスを取得していないと判定した場合、DRMコントローラ102は、ステップS74に進み、ライセンスサーバ13にライセンス取得要求を送信し、メインライセンスの送信を要求する。このとき、どのチャンネルのメインライセンスを要求するのかを表すチャンネル番号などの情報も、DRMコントローラ102からライセンスサーバ13に送信される。

【0133】

ステップS75において、DRMコントローラ102は、ライセンスを取得することに成功したか否かを判定する。DRMコントローラ102は、ステップS75において、メインライセンスを取得することに成功したと判定した場合、または、ステップS73でメインライセンスが取得済みであることがフラグに設定された場合、ステップS76に進み、メインライセンスを取得したことを通知するライセンス取得応答を受信機コントローラ101に送信し、処理を終了させる。

【0134】

一方、ステップS75において、ライセンスを取得することに成功していないと判定し

た場合、DRMコントローラ102は、ステップS77に進み、ライセンスサーバ13に対して行ったライセンスの要求の回数が、予め設定されているリトライ回数を超えたか否かを判定する。

【0135】

ステップS77において、リトライ回数を超えていないと判定した場合、DRMコントローラ102はステップS74に戻り、メインライセンスの送信を繰り返し要求する。また、ステップS77において、ライセンスの要求の回数がリトライ回数を超えたと判定した場合、DRMコントローラ102は、ステップS78に進み、要求されたチャンネルのメインライセンスを取得できなかったことをフラグに設定する（エラーを設定する）。このとき、DRMコントローラ102は、メインライセンスを取得できなかったことを通知するライセンス取得応答をステップS76において受信機コントローラ101に送信し、処理を終了させる。

【0136】

次に、図12のフローチャートを参照して、コンテンツの再生を制御するDRMコントローラ102のコンテンツ再生処理について説明する。なお、図12においては、再生が要求されるコンテンツは暗号化コンテンツ記憶部103に既に記憶されており、そのコンテンツを配信するチャンネルのメインライセンスも既に取得されているものとする。

【0137】

ステップS91において、DRMコントローラ102は、受信機コントローラ101から再生準備要求が送信されてきたか否かを判定し、送信されてきたと判定するまで待機する。図8および図9を参照して説明したように、コンテンツの再生がユーザから指示されたタイミングで受信機コントローラ101から再生準備要求が送信されてくる（図9のステップS45）。

【0138】

DRMコントローラ102は、ステップS91において、再生準備要求が送信されてきたと判定した場合、ステップS92に進む。

【0139】

ステップS92において、DRMコントローラ102は、再生が要求されたコンテンツに対応するサブライセンスをサブライセンス復号部106にセット（提供）し、ステップS93に進み、サブライセンス復号要求（図9のステップS47）を送信することで、その復号を行わせる。この要求に応じて、サブライセンス復号部106は、コンテンツ鍵記憶部108からコンテンツ鍵Kc1を読み出し、コンテンツ鍵Kc1を用いてサブライセンスを復号する。復号が成功したか否かは、サブライセンス復号部106から送信されるサブライセンス復号応答（図9のステップS49）により通知される。

【0140】

DRMコントローラ102は、ステップS94において、サブライセンス復号部106から送信されるサブライセンス復号応答に基づいてサブライセンスの復号が成功したか否かを判定し、成功していない（失敗した）と判定した場合、ステップS95に進み、エラー処理を行い、処理を終了させる。

【0141】

一方、DRMコントローラ102は、ステップS94において、サブライセンスの復号がサブライセンス復号部106において成功したと判定した場合、ステップS96に進む。

【0142】

ステップS96において、署名検証部110は、メインライセンスとサブライセンスの署名の検証を行う。すなわち、サブライセンス復号部106により、コンテンツ鍵Kc1を用いてサブライセンスが復号されることで取得される利用権利、識別情報、コンテンツ鍵Kc2と、それらの情報を元に計算された署名がDRMコントローラ102から署名検証部110に出力されている。署名検証部110は、署名の検証結果をDRMコントローラ102に知らせる。

【0143】

ステップS97において、DRMコントローラ102は、署名検証部110からの通知に基づいて、署名の検証が成功したか否かを判定し、失敗したと判定した場合、ステップS95に進み、エラー処理を行う。一方、DRMコントローラ102は、ステップS97において、署名の検証が成功したと判定した場合、ステップS98に進む。

【0144】

DRMコントローラ102は、ステップS98において、記憶部107からメインライセンスの利用権利を、サブライセンス復号部106からサブライセンスの利用権利をそれぞれ利用条件確認部109にセットさせる（利用条件確認部109に出力させる）。

【0145】

ステップS99において、DRMコントローラ102は、利用条件確認要求（図9のステップS51）を送信することで利用条件の確認を利用条件確認部109に要求する。利用条件確認部109においては、コンテンツの再生が許可されているか否かが判定され、その判定結果が利用条件確認応答（図9のステップS53）として送信されてくる。

【0146】

なお、メインライセンスとサブライセンスの利用権利は、コンテンツの再生中も利用条件確認部109により保持され、コンテンツの再生終了まで、利用条件の確認がリアルタイムで行われる。例えば、再生中であっても、利用条件を満たさなくなったことが利用条件確認部109により確認されたときは、その再生が中止される。

【0147】

DRMコントローラ102は、ステップS100において、利用条件確認部109から送信される利用条件確認応答に基づいて、コンテンツの再生が可能であるか否か、すなわち、利用条件を満たしているか否かを判定する。DRMコントローラ102は、利用条件を満たしていないため、コンテンツを再生することができないと判定した場合、ステップS95に進みエラー処理を行った後、処理を終了させる。このとき、利用条件を満たしていないため、コンテンツを再生することができないことをユーザに通知する画面が表示されるなどの処理が行われる。

【0148】

一方、ステップS100において、DRMコントローラ102は、コンテンツが再生可能であると判定した場合、すなわち、利用条件を満たしていることが利用条件確認部109により確認された場合、ステップS101に進み、コンテンツの再生が可能であることを通知する再生準備応答（図9のステップS55）を受信機コントローラ101に送信し、処理を終了させる。その後、受信機コントローラ101によりコンテンツの再生が管理される。

【0149】

次に、図13のフローチャートを参照して、図12の処理に続けて行われる受信機コントローラ101のコンテンツ再生処理について説明する。

【0150】

ステップS111において、受信機コントローラ101は、コンテンツの再生が可能であることがDRMコントローラ102から通知されてきたか否かを判定し、コンテンツの再生が不可能であることが通知されてきたと判定した場合、ステップS112に進み、エラー処理を行い、処理を終了させる。

【0151】

一方、受信機コントローラ101は、ステップS111において、コンテンツの再生が可能であることがDRMコントローラ102から通知されてきたと判定した場合、ステップS113に進み、サブライセンス復号部106を制御して、サブライセンスを復号したときに得られたコンテンツ鍵Kc2をコンテンツ復号部104にセットさせる。

【0152】

ステップS114において、受信機コントローラ101は、コンテンツ復号要求をコンテンツ復号部104に送信し（図9のステップS57）、サブライセンス復号部106から供給されるコンテンツ鍵Kc2を用いてコンテンツの復号を開始することを要求する。コ

ンテンツ復号部104においては、DRMコントローラ102からの要求に応じてコンテンツの復号が行われ、復号されたコンテンツが再生部105により再生される。コンテンツの再生が終了したとき、コンテンツ復号応答により、コンテンツの復号が終了したことがコンテンツ復号部104から受信機コントローラ101に通知される（図9のステップS59）。

【0153】

ステップS115において、受信機コントローラ101は、コンテンツの再生が終了したか否かを判定し、終了したと判定するまで待機する。

【0154】

受信機コントローラ101は、ステップS115において、コンテンツの再生が終了したと判定した場合、記憶部107に記憶されている利用状況、利用実績を再生部105により更新させ、処理を終了する。ここでは、メインライセンスで規定される利用条件の範囲内でのコンテンツの利用状況と、サブライセンスで規定される利用条件の範囲内でのコンテンツの利用状況の双方が1つのサービス名（チャンネル名）で関連付けられ、メインライセンスの利用状況として記録される。利用実績に関しても同様にサブライセンスで規定される利用条件に従った結果がメインライセンス内の利用実績に記録される。これにより、チャンネル単位で契約するサブスクリプションサービスの利用状況及び利用実績をメインライセンスで一括して管理することが可能になる。

【0155】

以上のように、メインライセンスとサブライセンスの2つのライセンスによって、1つのチャンネルで配信されるそれぞれのコンテンツに異なる利用条件を設定するなどの様々な利用条件を容易に規定することができる。すなわち、コンテンツ配信事業者は、2つのライセンスによりコンテンツの著作権を適切に保護しつつ、様々な形態のサービスを提供することができる。

【0156】

例えば、チャンネル毎の契約を行った後は、そのチャンネルで配信される全てのコンテンツが利用可能になるようなサービスはもちろん、チャンネル毎の契約を行った後でも、そのチャンネルで配信される、あるコンテンツには利用回数の制限を設定し、他のコンテンツには利用する毎に料金が発生するようなサービスなど、様々な形態のサービスを提供することができる。

【0157】

また、ユーザとしても、サブライセンスがコンテンツとともに送信されてくるため、メインライセンスを受信機15に予め取得させておけば、取得したコンテンツの再生を迅速に開始させることができる。すなわち、コンテンツの再生を開始させる前に受信機15からサーバにアクセスし、公開鍵証明書による認証を行わせるなどの処理を省くことができる。

【0158】

以上においては、受信機15においてライセンスの管理とコンテンツの再生の両方が行われるとしたが、受信機15が有するライセンスで規定される利用条件の範囲内での利用を許可するライセンスが、受信機15からDRM機能を有する他の機器に出力（エクスポート（export））され、その機器においてコンテンツの再生が行われるようにしてもよい。

【0159】

図14は、ライセンスのエクスポートについて示す図である。

【0160】

図14の例においては、受信機15は、あるチャンネルで配信されるコンテンツを合計3回利用することができることを規定するメインライセンス（図14においては、1回利用可能であることを規定するメインライセンスが3つ図示されている）と、そのチャンネルで配信されるコンテンツAの有効期限が2003年10月31日（2003/10/31）までであることを規定するサブライセンスA、同じチャンネルで配信されるコンテンツBが1回だけ利用可能であることを規定するサブライセンスBを有している。コンテンツAとコンテンツBは図1

4 の受信機 1 5 の暗号化コンテンツ記憶部 1 0 3 に記憶されている（図示せず）。

【0 1 6 1】

この状態で、例えば、メインライセンスの一部である 1 回分のコンテンツの利用を許可する利用権利と、サブライセンス A の利用権利（有効期限 2003/10/31）からライセンス A が生成され、ライセンス A が白抜き矢印 # 1 で示されるように DRM 機能を有する情報処理端末 1 2 1 にエクスポートされた場合、情報処理端末 1 2 1 においては、ライセンス A に基づいてコンテンツ A を利用することが可能になる。

【0 1 6 2】

すなわち、情報処理端末 1 2 1 においては、コンテンツ A を 2003 年 10 月 31 日までに 1 回だけ利用することが可能になる。なお、ライセンス A とともにコンテンツ A が受信機 1 5 から情報処理端末 1 2 1 に送信されるようにしてもよいし、コンテンツ A は、情報処理端末 1 2 1 自身がコンテンツサーバ 1 2 から取得するようにしてもよい。

【0 1 6 3】

一方、ライセンスをエクスポートした受信機 1 5 においては、コンテンツ（コンテンツ A、B）を合計 3 回利用可能であることを規定していたメインライセンスが、白抜き矢印 # 2 の先に示されるように、合計 2 回利用可能であることを規定するライセンスに更新される。すなわち、メインライセンスによる利用回数が、情報処理端末 1 2 1 にエクスポートした回数（1 回）だけ減算されたものに更新される。なお、サブライセンス A とサブライセンス B に変更はない。

【0 1 6 4】

このように、受信機 1 5 が取得したライセンスにより規定される利用条件の範囲内で、他の機器にコンテンツの利用が許可されるようにしてもよい。これにより、コンテンツの著作権の保護を図りつつ、比較的自由度の高いコンテンツの利用が可能になる。

【0 1 6 5】

以上のような利用可能回数や、利用可能累積時間などのユーザがコンテンツを利用することに依拠して、残りの利用条件が変化するライセンスの場合（利用回数がエクスポート毎に減っていくライセンス、エクスポート先での利用毎に利用可能な累積時間が減っていくライセンスの場合）、エクスポート元とエクスポート先のライセンスとで過不足が生じないようにすれば、ライセンスのエクスポートを許可することによってコンテンツの配信事業者が不利益を受けることは少ない。しかしながら、例えば、「2003 年 10 月 31 日まで利用可能」といった、期間を規定するライセンスの場合、受信機 1 5 からその期間内でコンテンツの利用が許可されるライセンスが複数発行されたときには、コンテンツの配信事業者が不利益を受けるおそれがあるため、この場合、エクスポートすることができる回数がライセンスの管理者（発行者）が許可する回数に制限されるようにしてもよい。

【0 1 6 6】

図 1 5 は、ライセンスの移動について示す図である。ここで、「移動」とは、あるコンテンツの利用条件を規定するライセンス全体が他の機器に出力されることをいう。

【0 1 6 7】

図 1 5 の例においては、受信機 1 5 は、あるチャンネルで配信されるコンテンツを 3 回だけ利用することが可能であることを規定するメインライセンスと、そのチャンネルで配信されるコンテンツ A を 2003 年 10 月 31 日（2003/10/31）まで利用可能であることを規定するサブライセンス A、同じチャンネルで配信されるコンテンツ B を 1 回だけ利用することが可能であることを規定するサブライセンス B を有している。

【0 1 6 8】

この状態で、例えば、メインライセンスの利用権利と、サブライセンス A そのものからライセンス A が生成され、白抜き矢印 # 2 1 で示されるようにライセンス A が情報処理端末 1 2 1 に移動された場合、情報処理端末 1 2 1 においては、ライセンス A に基づいてコンテンツ A を利用することが可能になる。すなわち、情報処理端末 1 2 1 においては、コンテンツ A を 2003 年 10 月 31 日まで合計 3 回利用可能になる。

【0 1 6 9】

この状態で、例えば、メインライセンスの利用権利3回のうち、1回が白抜き矢印#11で示されるように情報処理端末121に移動する。情報処理端末121においては、コンテンツサーバ12などからコンテンツAとサブライセンスAを取得することにより、コンテンツAを利用することができる。また、コンテンツBを利用したい場合も同様な手法を用いることで利用することができる。

【0170】

一方、ライセンスを移動させた受信機15においては、移動させたメインライセンスの利用権利1回が消去され、利用権利が2回となるように更新される。なお、移動後であっても、サブライセンスAとサブライセンスBに変更はない。

【0171】

このように、受信機15から他の機器にライセンスの移動が許可されることによっても、コンテンツの著作権の保護を図りつつ、比較的自由度の高いコンテンツの利用が可能となる。なお、DRMの方式が複数ある場合、ライセンスの移動は、同一のDRM方式を採用する機器間でのみ許可されるようにしてもよい。

【0172】

以上においては、ダウンロードするコンテンツ（またはストリーミングにより再生するコンテンツ）を指定してコンテンツサーバ12からコンテンツを取得するコンテンツ配信システムの場合について主に説明したが、コンテンツサーバ12からコンテンツがマルチキャストされるコンテンツ配信システムの場合にも本発明は適用することができる。

【0173】

図16は、マルチキャストにより配信されるコンテンツの例を示す図である。マルチキャストによるコンテンツ配信においては、配信事業者が管理するスケジュールに沿ってコンテンツが時間的に連続して配信される。

【0174】

図16の例においては、コンテンツA乃至Dが、その順番でチャンネル#1により配信されており、例えば、ユーザが時刻t1でチャンネル#1にアクセス（サーバにアクセス）した場合、コンテンツAを途中から利用することができ、時刻t2でチャンネル#1にアクセスした場合、コンテンツCを途中から利用することができる。

【0175】

このようなマルチキャストによるコンテンツ配信システムにおいて、上述したように、メインライセンスと、コンテンツとともに配信されるサブライセンスによりそれぞれのコンテンツの利用条件が規定される場合、受信機15は、例えば、コンテンツAの配信が開始される時刻t11にチャンネル#1にアクセスしているとき、コンテンツAの再生を開始する前に、メインライセンスと、時刻t11以降にコンテンツAとともに配信されるサブライセンスにより利用条件の確認を行う必要がある。そして、受信機15は、メインライセンスとサブライセンスにより規定される利用条件をいずれも満たすことを確認してからコンテンツAを再生する。

【0176】

また、受信機15は、例えば、コンテンツAの配信が終了され、コンテンツAに続くコンテンツBの配信が開始される時刻t12になったとき、コンテンツBの再生を開始する前に、メインライセンスと、時刻t12以降にコンテンツBとともに配信されるサブライセンスにより利用条件の確認を行い、メインライセンスとサブライセンスにより規定される利用条件をいずれも満たすことを確認してからコンテンツBを出力する。配信されるコンテンツが切り替わる他の時刻t13乃至t15でも同様である。

【0177】

従って、マルチキャストによるコンテンツ配信システムにおいては、上述したように、コンテンツとともに、そのコンテンツの利用条件を規定するサブライセンスが配信される場合、シームレスなコンテンツの出力を行うことができない。すなわち、コンテンツAの出力が終了してからコンテンツBの出力が開始される、コンテンツBの利用条件の確認を行っている間はコンテンツを出力することができない。

【0178】

そこで、先に配信される第1のコンテンツのサブライセンスと、第1のコンテンツに続けて配信される第2のコンテンツのサブライセンスとが、第1のコンテンツとともに配信されるようにし、第1のコンテンツの配信中に、第2のコンテンツのサブライセンスが受信機15に予め提供されるようにすることで、シームレスなコンテンツの出力を確保するようにしてもよい。

【0179】

図17は、先に配信される第1のコンテンツのサブライセンスと、第1のコンテンツに続けて配信される第2のコンテンツのサブライセンスとが、第1のコンテンツとともに配信されるコンテンツ配信について示す図である。

【0180】

図17の例においては、コンテンツA乃至Cが時間的に連続してチャンネル#1により配信されており、その順番で受信機15により受信される。

【0181】

コンテンツAは、コンテンツAに対応するサブライセンス（Evenに対応するサブライセンス）と、コンテンツAに続けて配信されるコンテンツBに対応するサブライセンス（Oddに対応するサブライセンス）とともに配信データにより配信される。コンテンツAには「Even」のフラグが割り振られており、コンテンツAを構成する各パケットには「Even」のフラグが設定される。

【0182】

受信機15は、コンテンツAを再生する場合、フラグの設定から、対応するコンテンツAのサブライセンスを用いて、そのサブライセンスとメインライセンスによりコンテンツAの利用が許可されているか否かを確認する。受信機15は、コンテンツAの再生が許可されていることを確認したとき、コンテンツAを再生する。

【0183】

また、受信機15は、コンテンツAを再生している間（コンテンツAの配信中）、コンテンツAとともに配信されるコンテンツBのサブライセンスとメインライセンスに基づいて、コンテンツAに続けて配信されるコンテンツBの利用が許可されるか否かを確認する。すなわち、コンテンツAの配信中に、次に配信されるコンテンツBの利用が許可されているか否かが予め確認される。

【0184】

コンテンツAの配信が終了し、コンテンツBの配信が開始されたとき、受信機15は、パケットのフラグが「Even」から「Odd」に切り替わることに応じて、用いるライセンスをコンテンツBに対応するサブライセンスに切り替えとともに、コンテンツBの出力を開始させる。

【0185】

このように、続けて配信されるコンテンツのサブライセンスが、先に配信されるサブライセンスとともに受信機15に提供されるようにすることにより、受信機15は、続けて配信されるコンテンツの利用条件を予め確認することができ、シームレスなコンテンツの出力を確保することができる。

【0186】

なお、図17の例においては、コンテンツBとともに、コンテンツBのサブライセンスと、コンテンツBの次に配信されるコンテンツCのサブライセンスが配信されている。また、コンテンツCとともにコンテンツCのサブライセンスが配信されている。

【0187】

また、以上においては、コンテンツAとともに、コンテンツAのサブライセンスと、コンテンツBのサブライセンス（コンテンツB全体のサブライセンス）が提供されたとしたが、コンテンツAとともに、コンテンツA全体のサブライセンスと、コンテンツBのサブライセンス内に、さらに、開始後数秒間の部分の利用条件を規定するサブライセンスが提供されるようにしてもよい。

【0188】

この場合、コンテンツAの再生開始時には、提供されているコンテンツA全体の利用条件に基づいて、コンテンツAの再生が可能であるか否かが確認され、コンテンツAの再生が可能であるときには、上述したようにして再生部105によりコンテンツAが再生される。このとき、コンテンツAのコンテンツ鍵Kc2がコンテンツ復号部104に供給されている。

【0189】

さらに、コンテンツAの再生中には、コンテンツBの開始後数秒間の部分のみの利用条件に基づいて、コンテンツBの開始後数秒間の部分のみの再生が可能であるか否かが確認され、コンテンツBの開始後数秒間の部分のみの再生が可能である場合には、再生部105によりコンテンツBの開始後数秒間の部分のみがコンテンツAの再生終了後に継続して再生される。

【0190】

コンテンツAの再生中に、コンテンツの切り替わりを示すフラグが「Even」から「Odd」に変わったとき、コンテンツAの再生停止が指示され、コンテンツBの開始後数秒間の部分の再生が許可されていることが予め確認されていた場合には、コンテンツBのコンテンツ鍵Kc2に基づいてその部分の再生が行われる。これにより、コンテンツAに続けてコンテンツBをシームレスに再生させることができる。

【0191】

また、コンテンツAの再生停止が指示されたときには、コンテンツB全体の利用条件が利用条件確認部109に供給され、コンテンツBの数秒間の部分を再生している間に、その全体の利用条件が確認され、再生中の数秒間のコンテンツBの再生に続けて、コンテンツB全体の再生が開始される。

【0192】

同様の処理がコンテンツCについても行われる。すなわち、コンテンツB（コンテンツBの全体）の再生中に、そのときには提供されているコンテンツCの開始後数秒間の部分のみの利用条件を規定するサブライセンスが確認され、コンテンツBの再生が終了したとき、コンテンツCの部分的な再生が開始される。

【0193】

ここで、図18のフローチャートを参照して、図17のコンテンツが配信される場合に、それぞれのコンテンツをシームレスに再生する受信機15の処理について説明する。

【0194】

例えば、コンテンツAの配信が開始されるタイミングでチャネル#1にアクセスした場合、受信機15の受信機コントローラ101は、ステップS131において、コンテンツAのサブライセンスと、コンテンツAに続けて配信されるコンテンツBのサブライセンスをコンテンツAとともに取得する。この場合、コンテンツA、コンテンツAの利用条件を規定するサブライセンス、コンテンツBの利用条件を規定するサブライセンスを含む配信データが受信機コントローラ101により受信される。

【0195】

ステップS132において、DRMコントローラ102は、メインライセンスと、コンテンツAのサブライセンスにより規定される利用条件を利用条件確認部109に確認させる。すなわち、受信機コントローラ101により受信されたコンテンツAのサブライセンスは、サブライセンス復号部106によりコンテンツ鍵Kc1が用いられて復号され、利用条件確認部109に出力される。

【0196】

コンテンツAの利用が許可されている場合、ステップS133において、受信機コントローラ101はコンテンツ復号部104等を制御してコンテンツAを出力させる。これにより、ユーザはコンテンツAを利用することができる。

【0197】

コンテンツAの出力が行われている間、ステップS134において、DRMコントローラ

102は、メインライセンスと、コンテンツBのサブライセンスにより規定される利用条件をコンテンツBの配信が開始される前に利用条件確認部109に予め確認させる。

【0198】

ステップS135において、受信機コントローラ101は、コンテンツAの配信が終了したか否かを判定し、終了したと判定するまで待機し、コンテンツAの出力を続行させる。一方、受信機コントローラ101は、コンテンツAの配信が終了したとステップS135において判定した場合、ステップS136に進む。

【0199】

ステップS136以降の処理は、上述したステップS131乃至S135の処理と同様である。すなわち、ステップS136において、受信機コントローラ101は、コンテンツBのサブライセンス、コンテンツBに続けて配信されるコンテンツCのサブライセンスとともにコンテンツBを取得する。

【0200】

DRMコントローラ102は、ステップS137において、ステップS134で行われた確認の結果によりコンテンツBの利用が許可されている場合、コンテンツ復号部104等を制御し、コンテンツBを出力させる。このように、コンテンツBの利用が許可されているか否かは、コンテンツBの配信が開始される前に予め確認されているため、コンテンツAの配信が終了してからそれを行う必要はなく、コンテンツAに続けてコンテンツBを出力させることができる。

【0201】

コンテンツBの出力が行われている間、ステップS138において、DRMコントローラ102は、メインライセンスと、コンテンツCのサブライセンスにより規定される利用条件を、コンテンツCの配信が開始される前に利用条件確認部109に予め確認させる。

【0202】

ステップS139において、受信機コントローラ101は、コンテンツBの配信が終了したか否かを判定し、終了したと判定するまで待機し、コンテンツBの出力を続行させる。

【0203】

一方、受信機コントローラ101は、コンテンツBの配信が終了したとステップS139において判定した場合、ステップS140に進み、コンテンツCを、コンテンツCのサブライセンスとともに取得する。

【0204】

DRMコントローラ102は、ステップS141において、ステップS138で行われた確認の結果によりコンテンツCの利用が許可されている場合、コンテンツ復号部104等を制御してコンテンツCを出力させる。これにより、コンテンツBに続けてコンテンツCが出力される。

【0205】

ステップS142において、受信機コントローラ101は、コンテンツCの配信が終了したか否かを判定し、終了したと判定するまで待機する。ステップS142において、コンテンツCの配信が終了したと判定された場合、処理は終了される。

【0206】

以上の処理と同様の処理が、他のコンテンツがマルチキャストされる場合にも行われ、シームレスなコンテンツの出力が確保される。

【0207】

なお、以上においては、コンテンツの配信は、インターネット11を介して行われるとしたが、BS(Broadcasting Satellite)放送、CS(Communications Satellite)放送、地上デジタル放送を介して行われるようにしてもよい。

【0208】

上述した一連の処理は、ハードウェアにより実行させることもできるが、ソフトウェアにより実行させることもできる。この場合、そのソフトウェアを実行させる装置は、例え

ば、図 19 に示されるようなパーソナルコンピュータにより構成される。

【0209】

図 19 において、CPU(Central Processing Unit) 151 は、ROM(Read Only Memory) 152 に記憶されているプログラム、または、記憶部 158 から RAM(Random Access Memory) 153 にロードされたプログラムに従って各種の処理を実行する。RAM 153 にはまた、CPU 151 が各種の処理を実行する上において必要なデータなどが適宜記憶される。

【0210】

CPU 151、ROM 152、および RAM 153 は、バス 154 を介して相互に接続されている。このバス 154 にはまた、入出力インタフェース 155 も接続されている。

【0211】

入出力インタフェース 155 には、キーボード、マウスなどよりなる入力部 156、CRT(Cathode Ray Tube)、LCD(Liquid Crystal Display)などよりなるディスプレイ、並びにスピーカなどよりなる出力部 157、ハードディスクなどより構成される記憶部 158、インターネット 11 を介しての通信を行う通信部 159 が接続されている。

【0212】

入出力インタフェース 155 にはまた、必要に応じてドライブ 160 が接続され、磁気ディスク、光ディスク、光磁気ディスク、或いは半導体メモリなどからなるリムーバブルメディア 161 が適宜装着され、それから読み出されたコンピュータプログラムが、必要に応じて記憶部 158 にインストールされる。

【0213】

一連の処理をソフトウェアにより実行させる場合には、そのソフトウェアを構成するプログラムがネットワークや記録媒体からインストールされる。

【0214】

この記録媒体は、図 19 に示されるように、装置本体とは別に、ユーザにプログラムを提供するために配布される、プログラムが記録されている磁気ディスク（フレキシブルディスクを含む）、光ディスク（CD-ROM、DVD(Digital Versatile Disk)を含む）、光磁気ディスク（MD（登録商標）(Mini-Disk)を含む）、もしくは半導体メモリなどよりなるリムーバブルメディア 161 により構成されるだけでなく、装置本体に予め組み込まれた状態でユーザに提供される、プログラムが記録されている ROM 152 や、記憶部 158 などで構成される。

【0215】

なお、本明細書において、記録媒体に記録されるプログラムを記述するステップは、記載された順序に従って時系列的に行われる処理はもちろん、必ずしも時系列的に処理されなくとも、並列的あるいは個別に実行される処理をも含むものである。

【0216】

また、本明細書において、システムとは、複数の装置により構成される装置全体を表わすものである。

【図面の簡単な説明】

【0217】

【図 1】 本発明を適用したコンテンツ配信システムの構成例を示す図である。

【図 2】 サプライセンスとメインライセンスの関係を示す図である。

【図 3】 メインライセンスとサプライセンスに含まれる情報の例を示す図である。

【図 4】 図 1 のコンテンツサーバとライセンスサーバの機能構成例を示すブロック図である。

【図 5】 図 1 の受信機の機能構成例を示すブロック図である。

【図 6】 ライセンスサーバのライセンス生成処理について説明するフローチャートである。

【図 7】 コンテンツサーバの配信データ生成処理について説明するフローチャートである。

【図 8】 コンテンツサーバ、ライセンスサーバ、および受信機の間で行われる処理に

ついて説明するフローチャートである。

【図 9】コンテンツサーバ、ライセンスサーバ、および受信機の間で行われる処理について説明する、図 8 に続くフローチャートである。

【図 10】メインライセンスとサブライセンスの具体例を示す図である。

【図 11】DRMコントローラのライセンス取得処理について説明するフローチャートである。

【図 12】DRMコントローラのコンテンツ再生処理について説明するフローチャートである。

【図 13】受信機コントローラのコンテンツ再生処理について説明するフローチャートである。

【図 14】ライセンスのエクスポートについて示す図である。

【図 15】ライセンスの移動について示す図である。

【図 16】マルチキャストにより配信されるコンテンツの例を示す図である。

【図 17】マルチキャストにより配信されるコンテンツの他の例を示す図である。

【図 18】受信機のコンテンツ再生処理について説明するフローチャートである。

【図 19】パーソナルコンピュータの構成例を示すブロック図である。

【符号の説明】

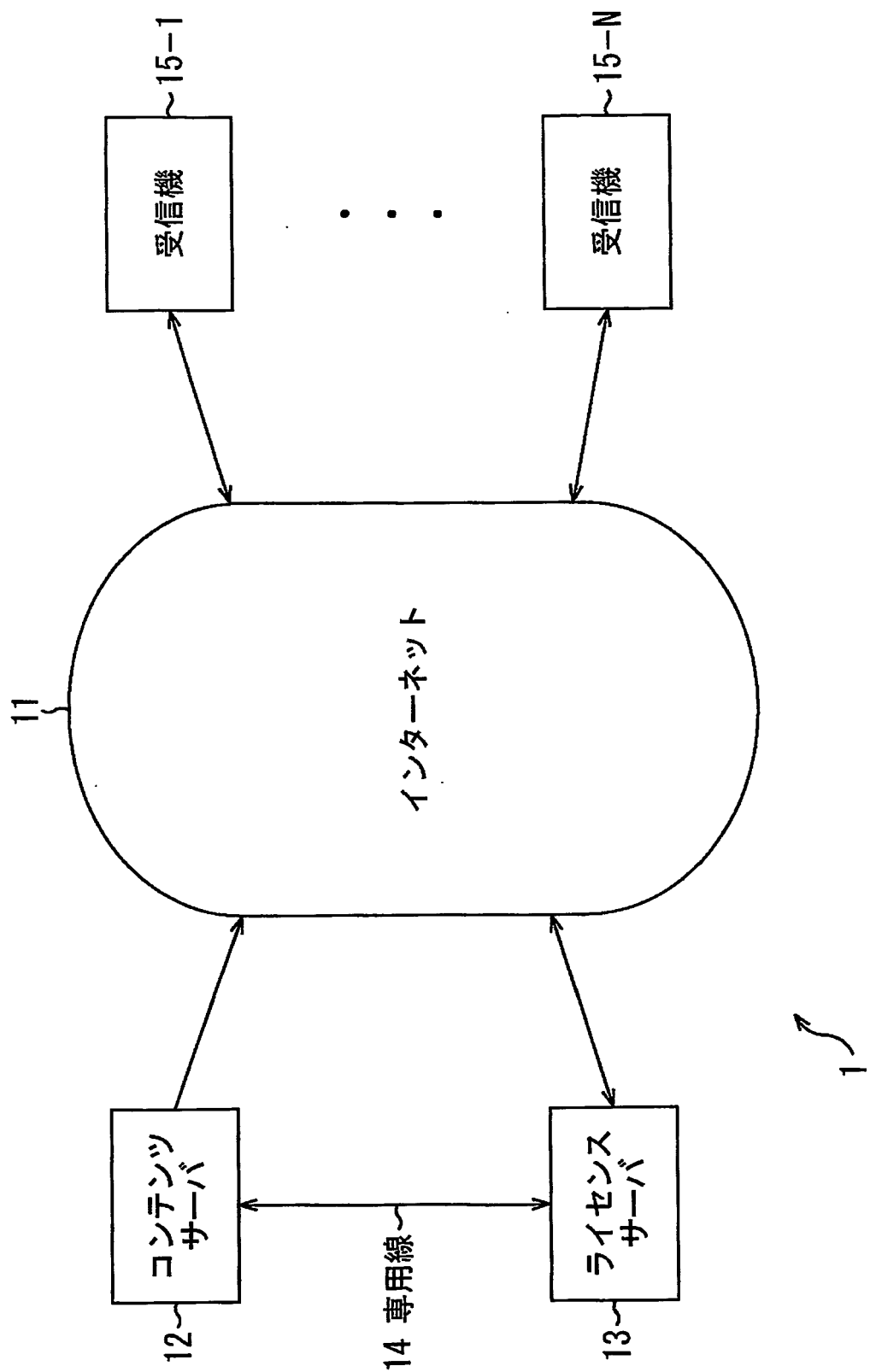
【0218】

1 コンテンツ配信システム, 11 インターネット, 12 コンテンツサーバ,
13 ライセンスサーバ, 15-1乃至15-N 受信機, 61 コンテンツ取得
部, 62 暗号化部, 63 配信データ生成部, 64 配信データ記憶部, 65
配信部, 81 コンテンツ鍵取得部, 82 情報取得部, 83 暗号化部, 8
4 署名生成部, 85 サブライセンス生成部, 86 コンテンツ鍵取得部, 87
情報取得部, 88 メインライセンス生成部, 89 メインライセンス提供部,
101 受信機コントローラ, 102 DRMコントローラ, 103 暗号化コンテン
ツ記憶部, 104 コンテンツ復号部, 105 再生部, 106 サブライセンス
復号部, 107 記憶部, 108 コンテンツ鍵記憶部, 109 利用条件確認部
, 121 情報処理端末

【書類名】 図面

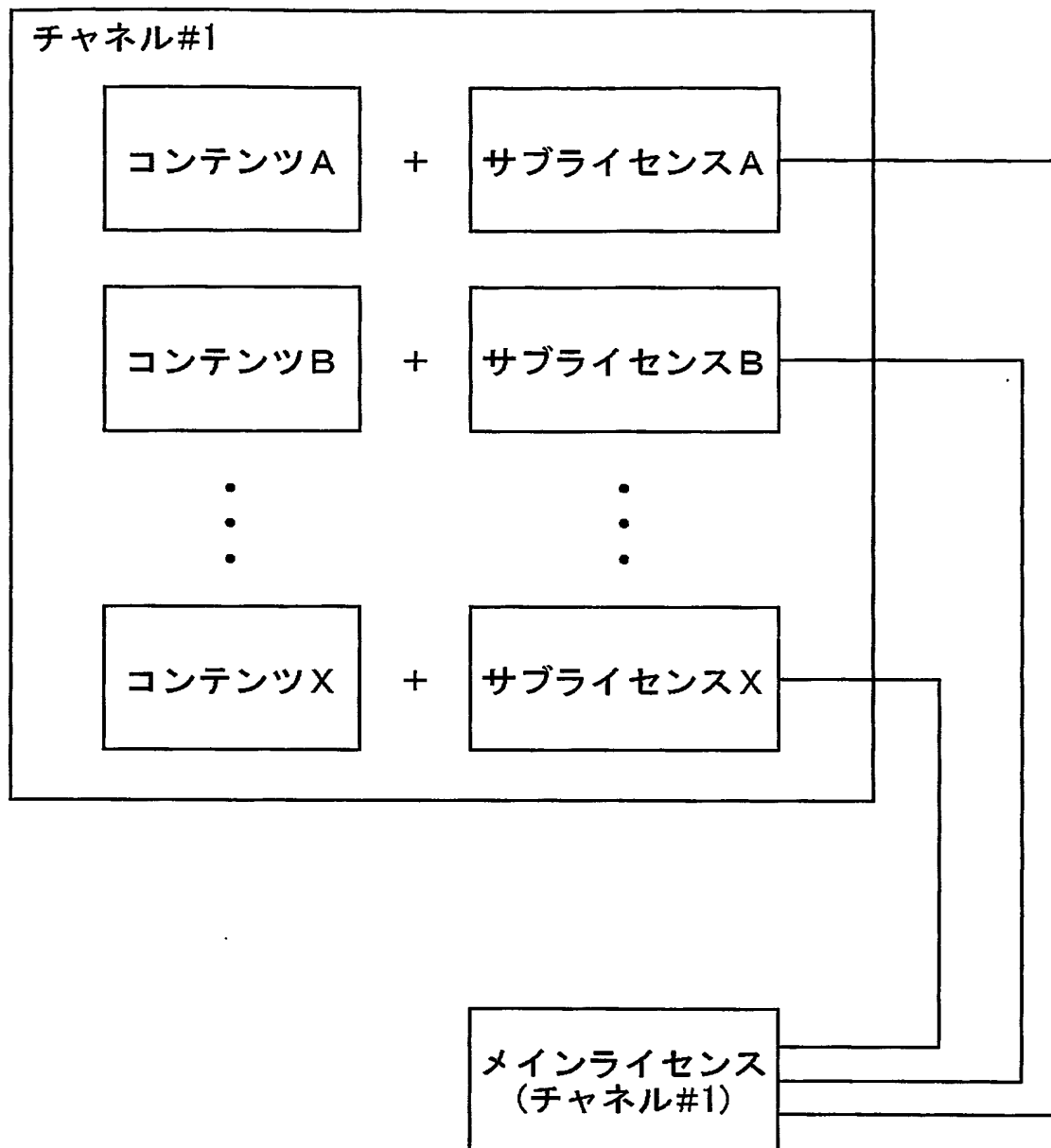
【図 1】

図 1



【図 2】

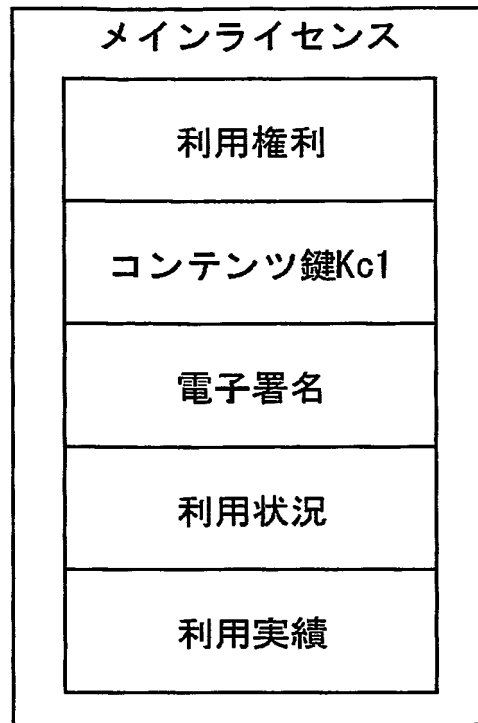
図2



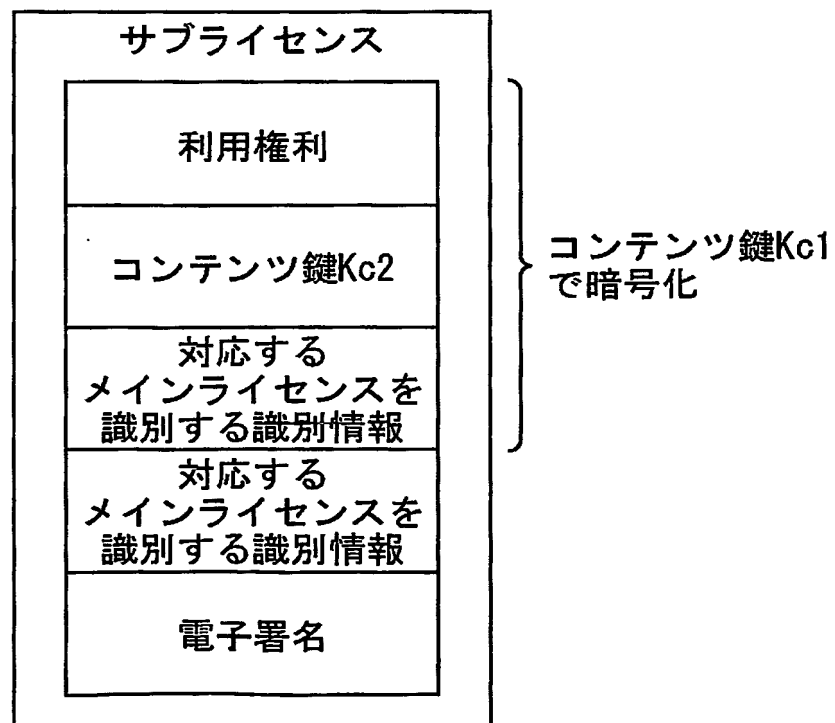
【図3】

図3

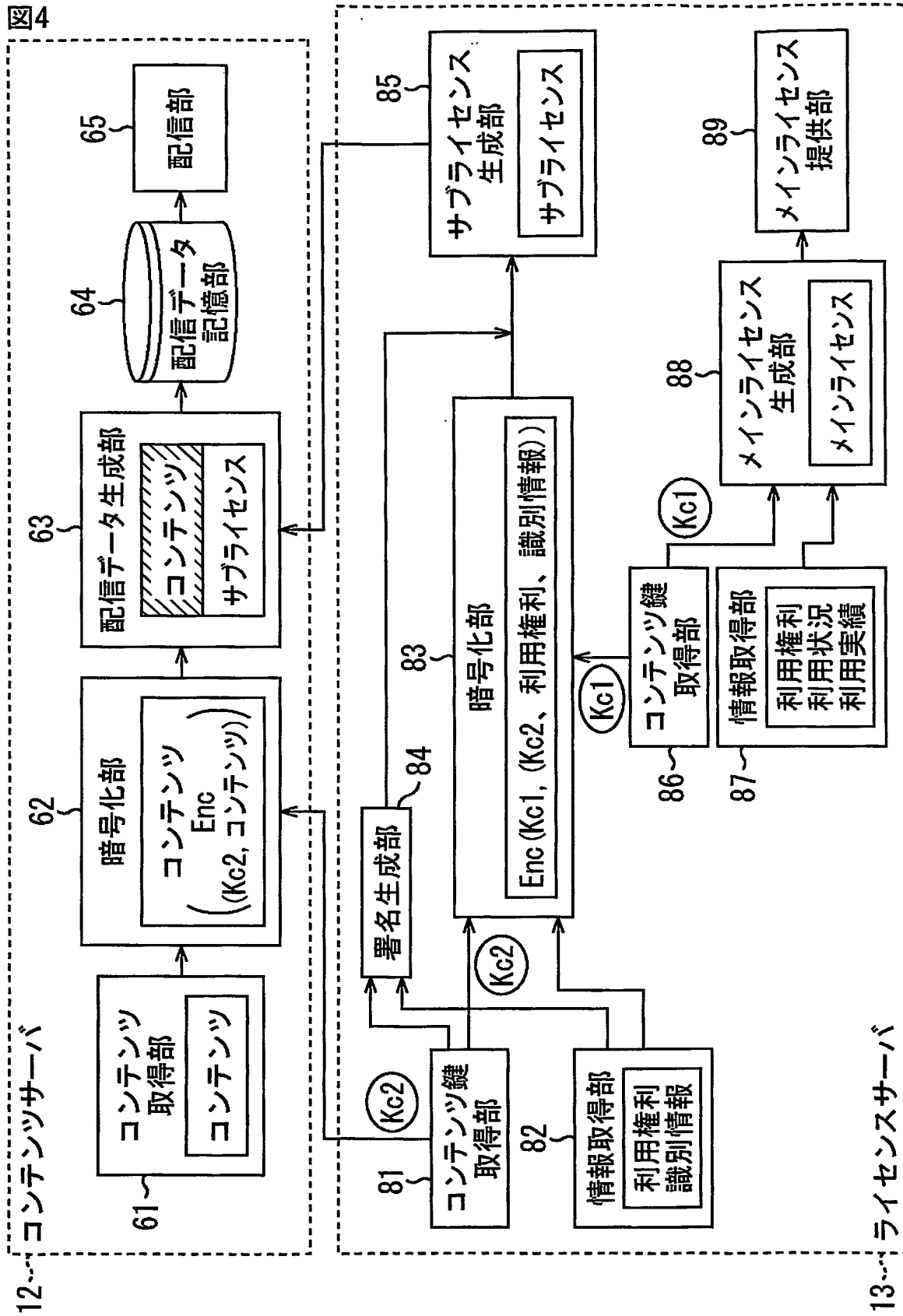
A



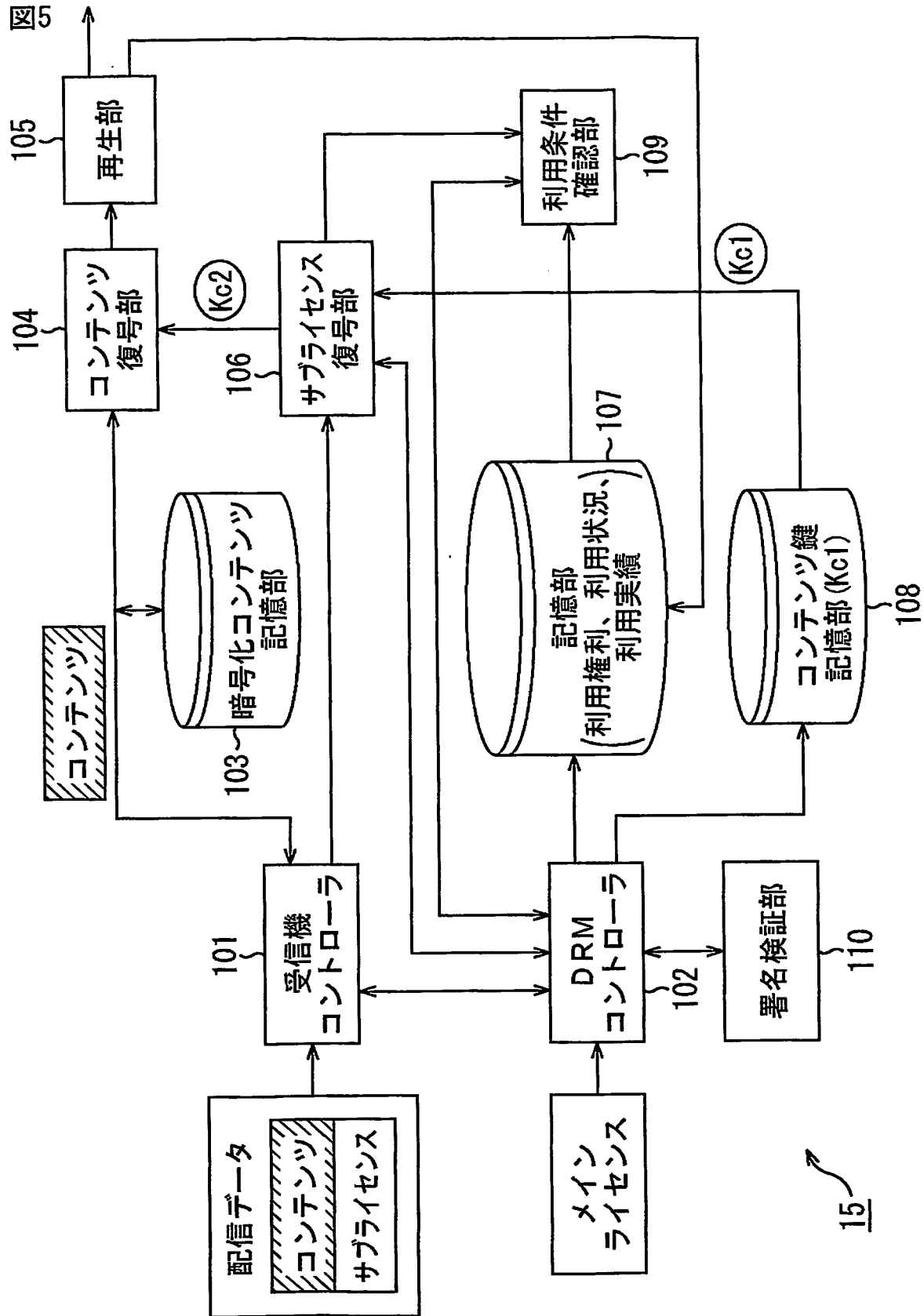
B



【図 4】

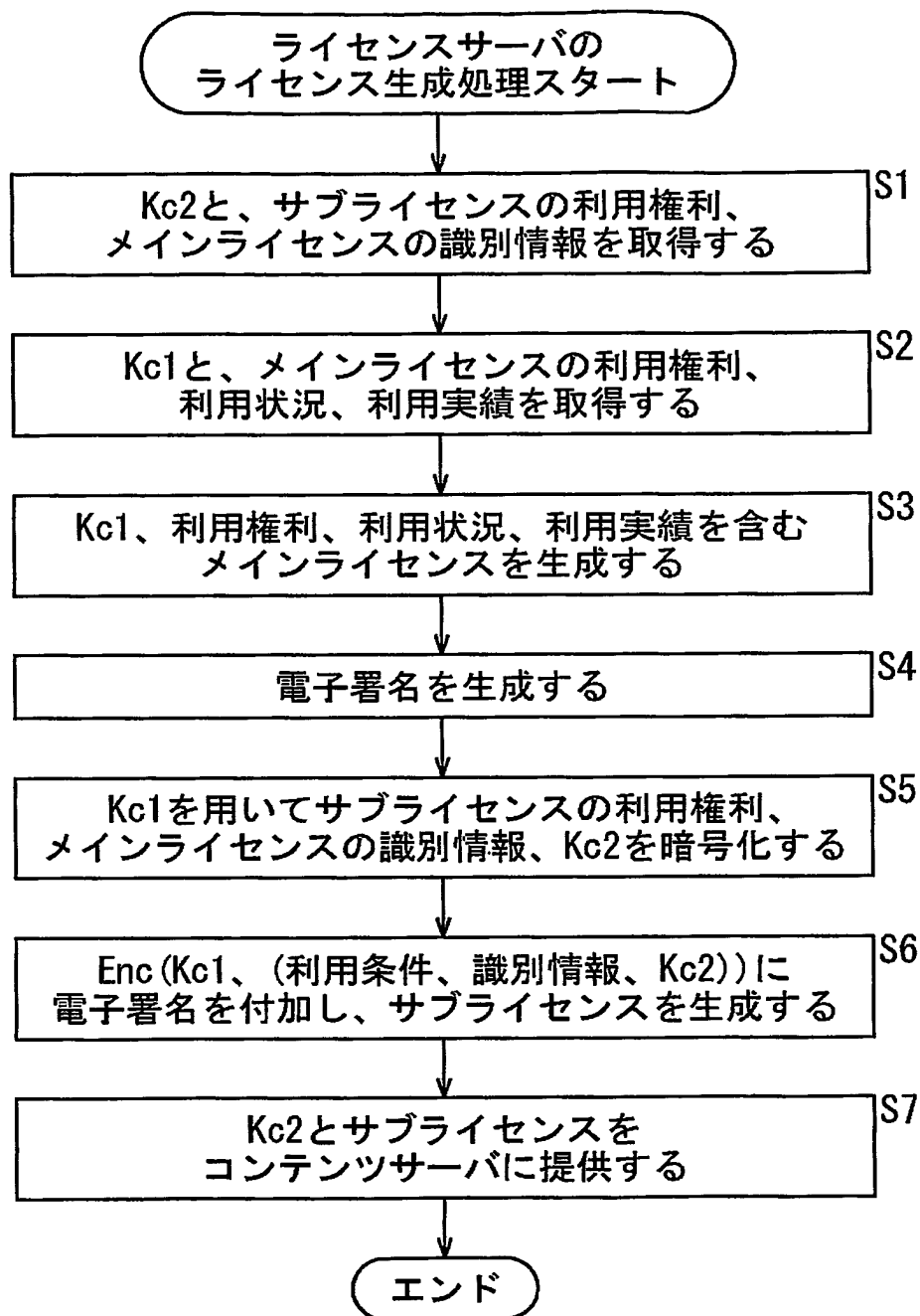


【図 5】

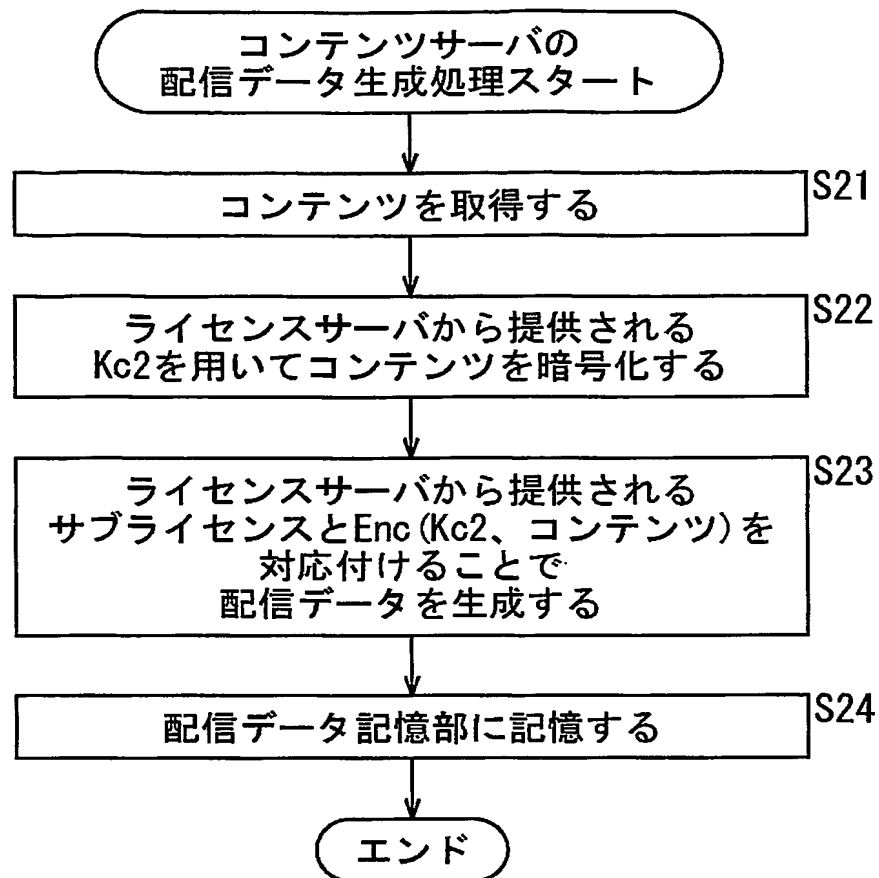


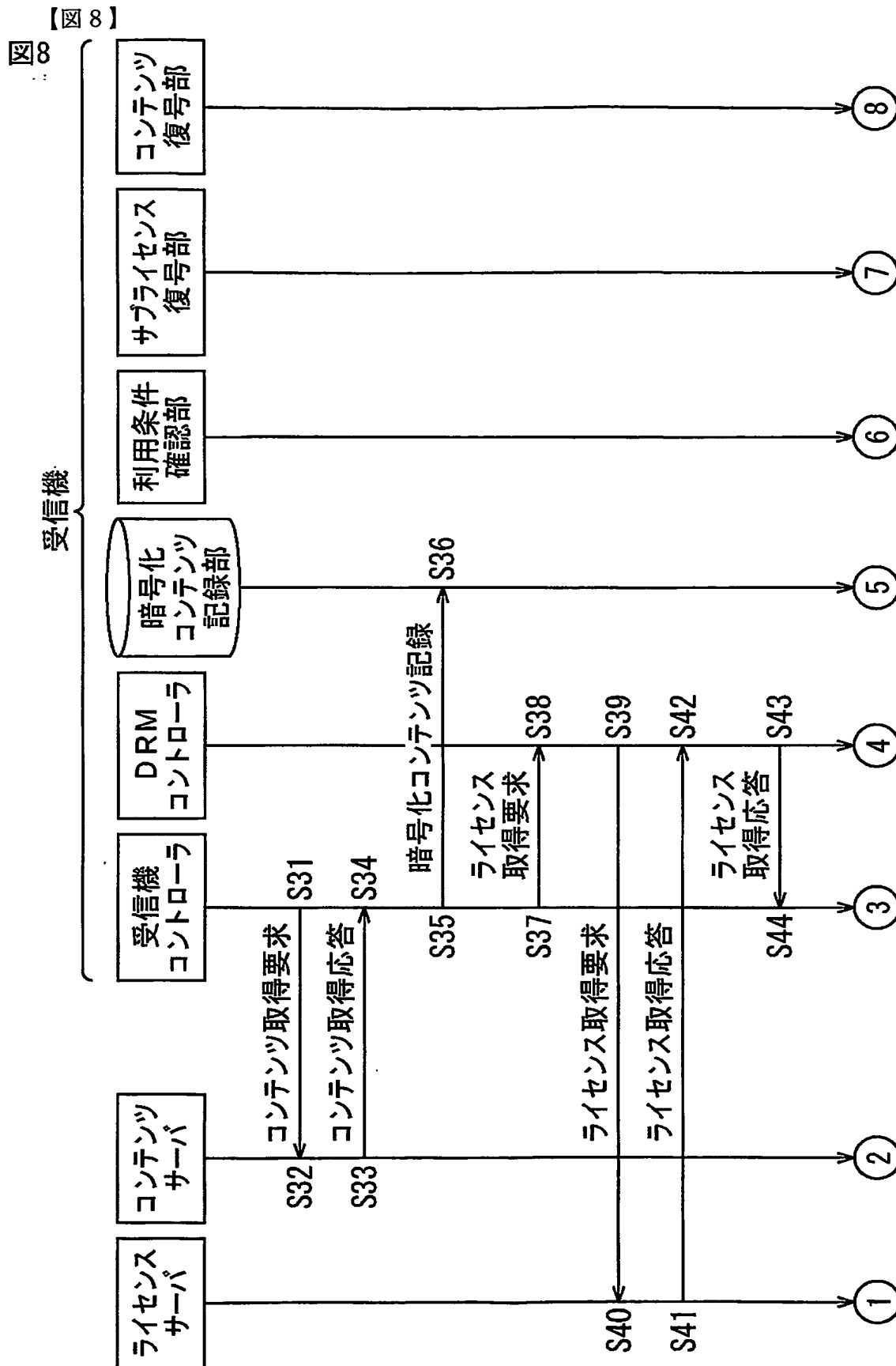
【図6】

図6



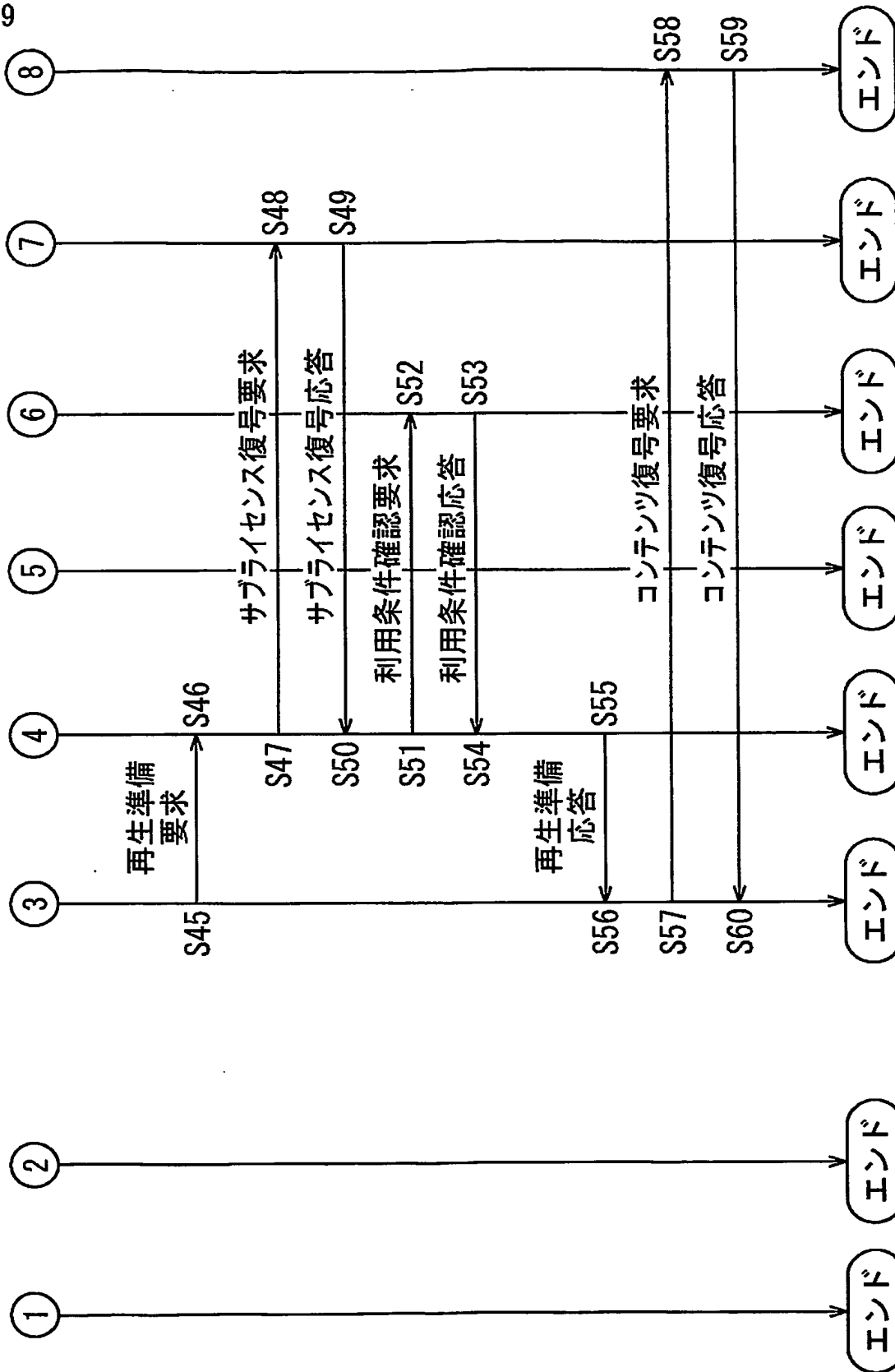
【図7】
図7





【図 9】

図9



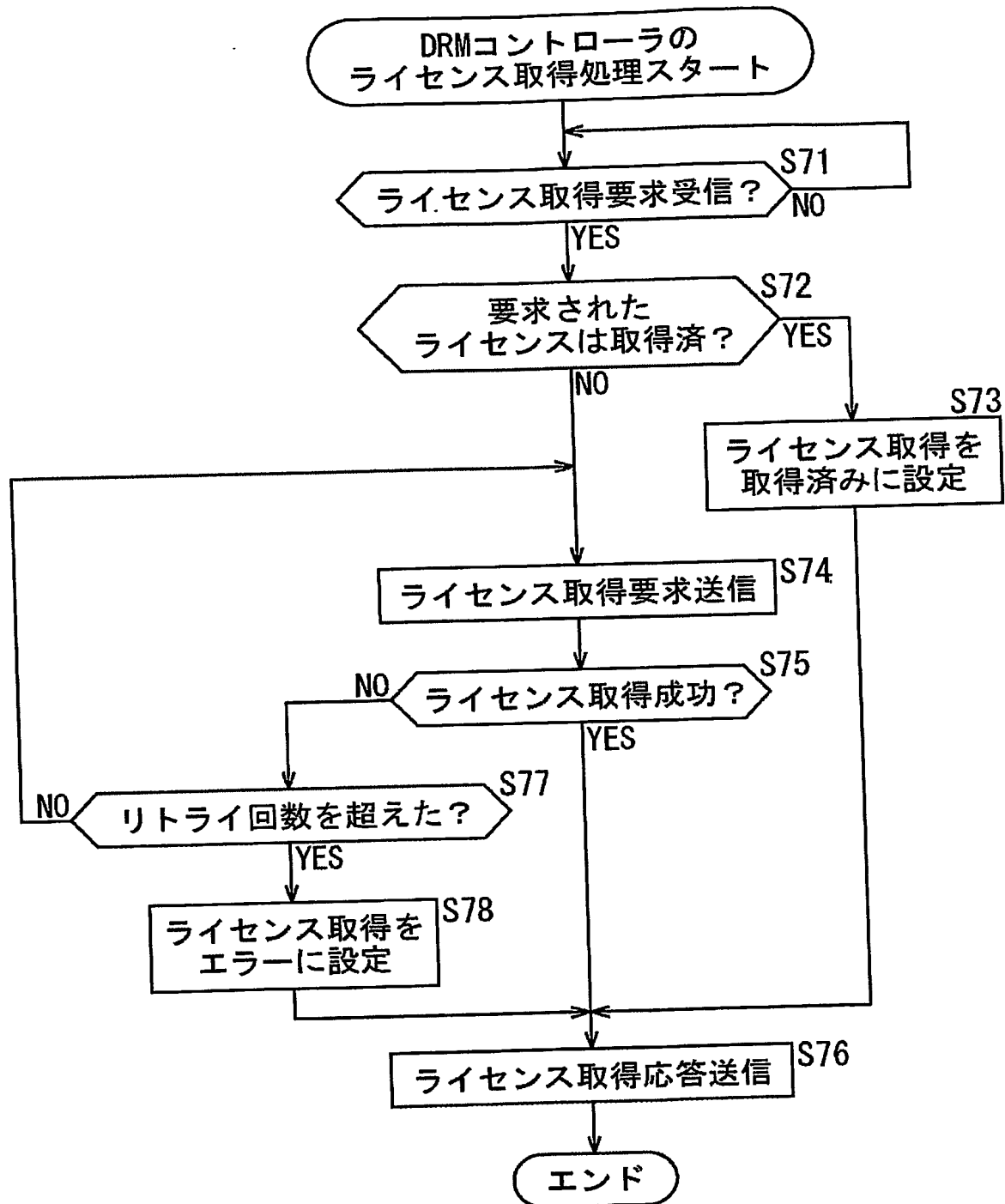
【図 10】

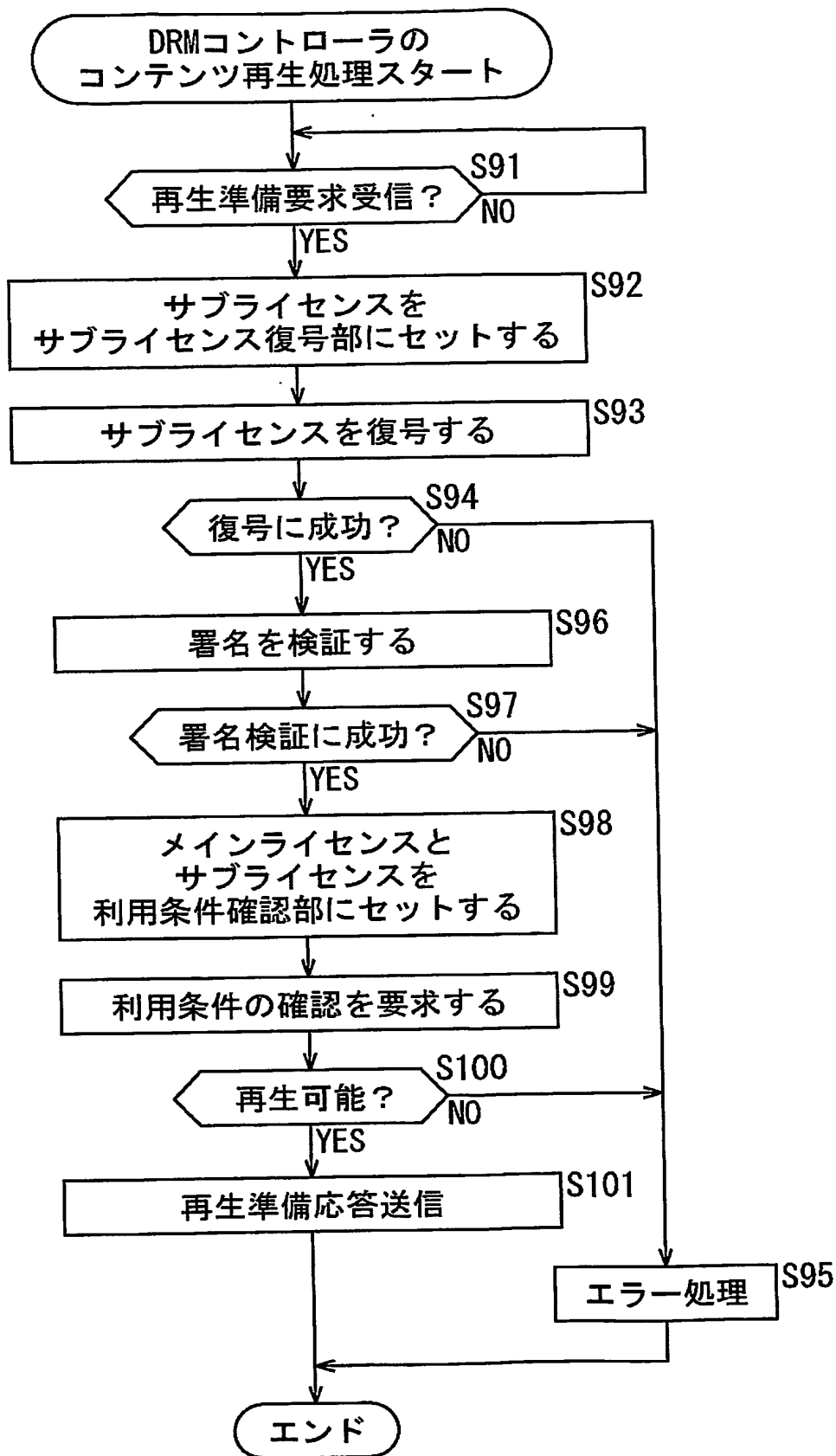
図10

	メインライセンス	サブライセンス	確認する利用条件
コンテンツA	有効期間 2003/10/01から 2003/10/31まで	10回利用可能	有効期間 2003/10/01から 2003/10/31まで 10回利用可能
コンテンツB	有効期間 2003/12/31まで	—	有効期間 2003/12/31まで

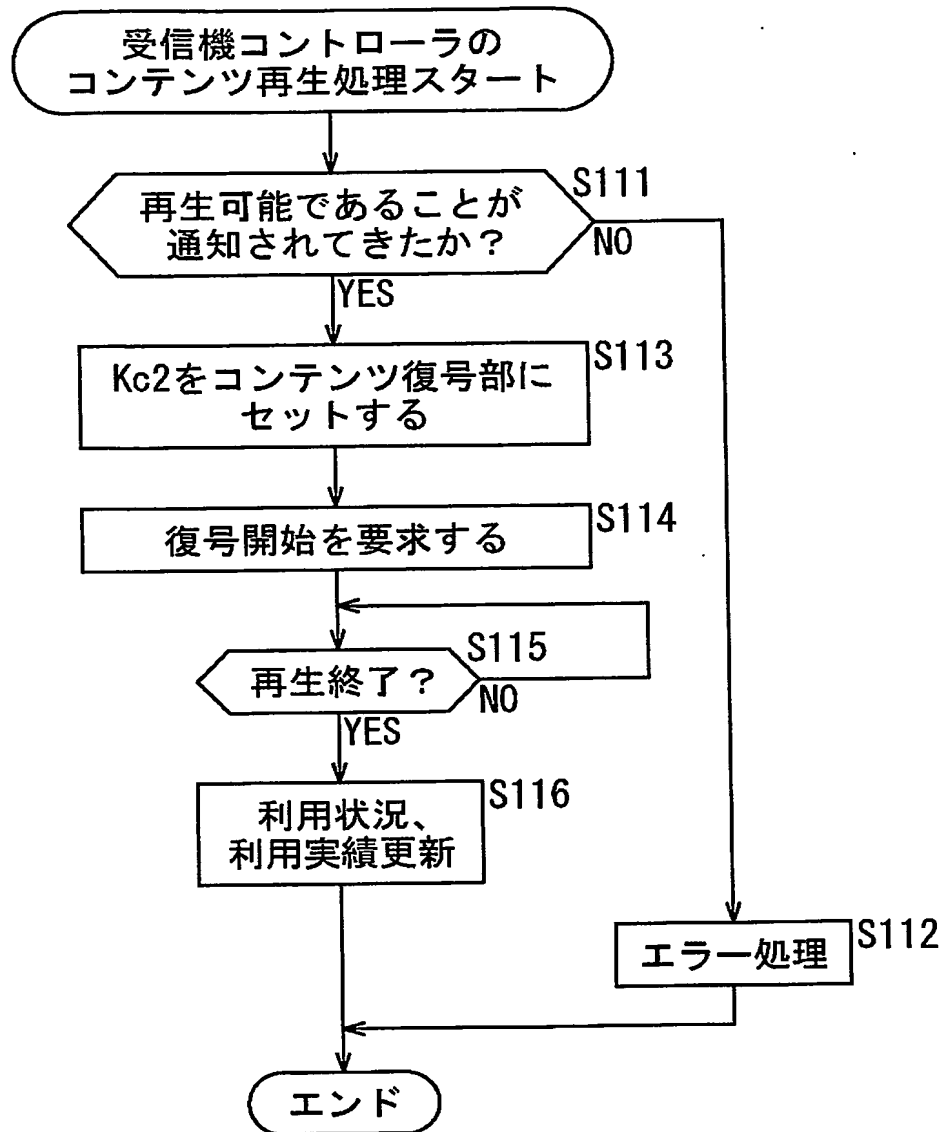
【図11】

図11

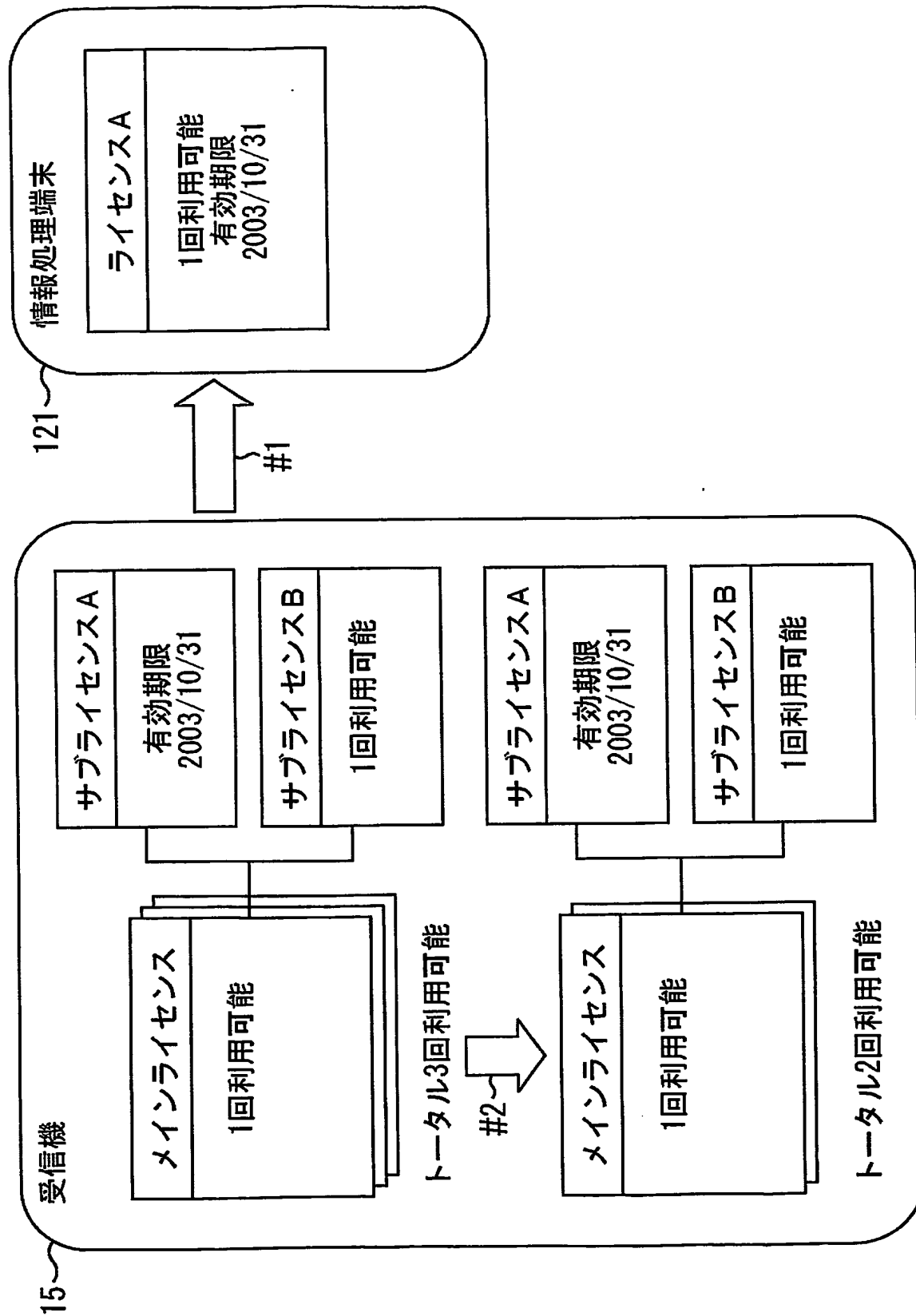


【図12】
図12

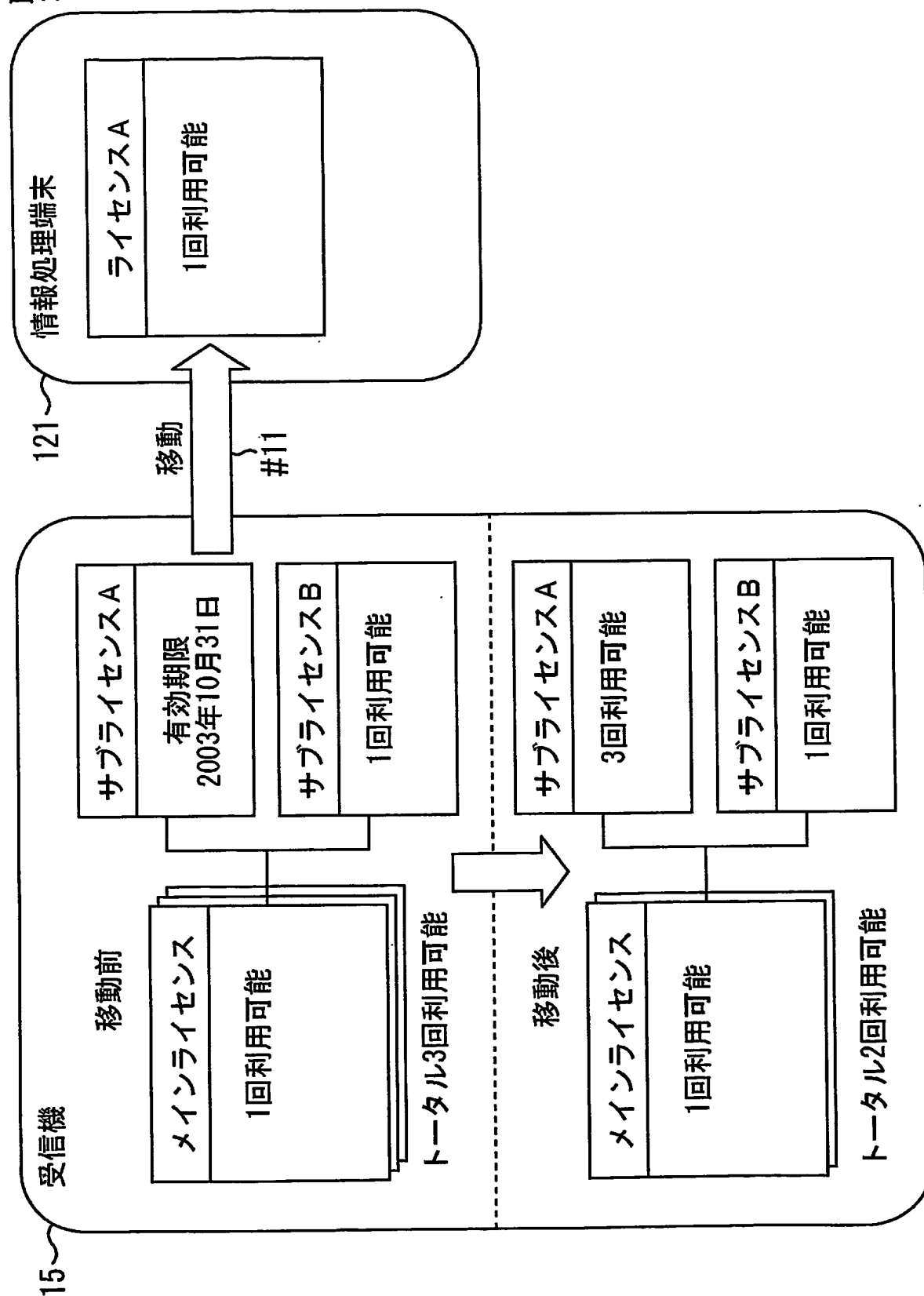
【図13】
図13



【図 14】
図 14

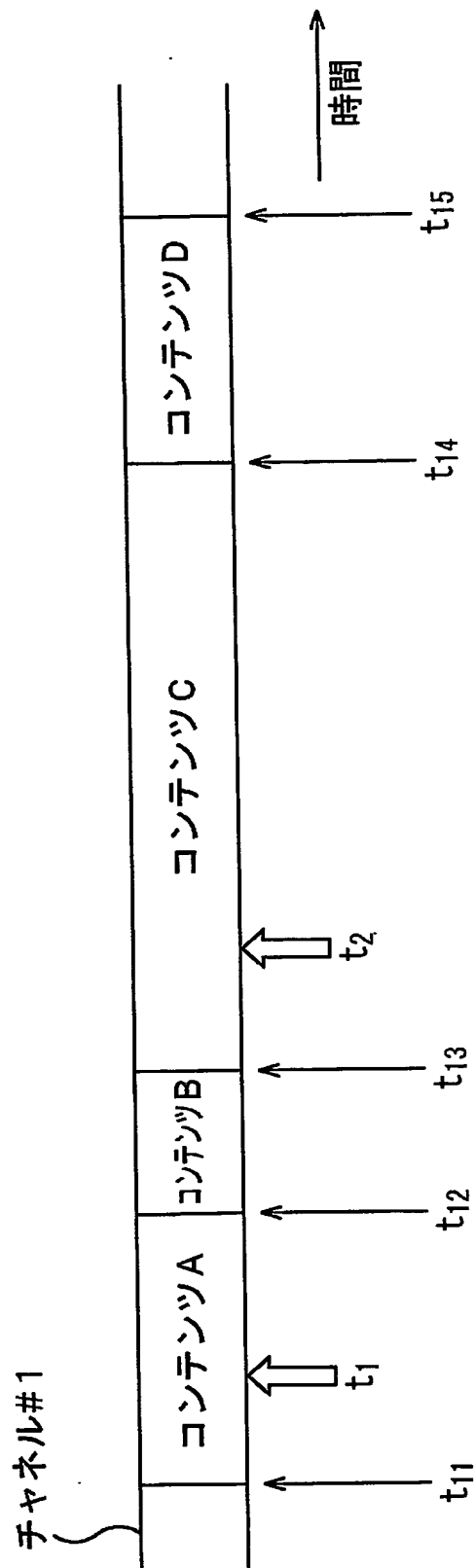


【図15】
図15

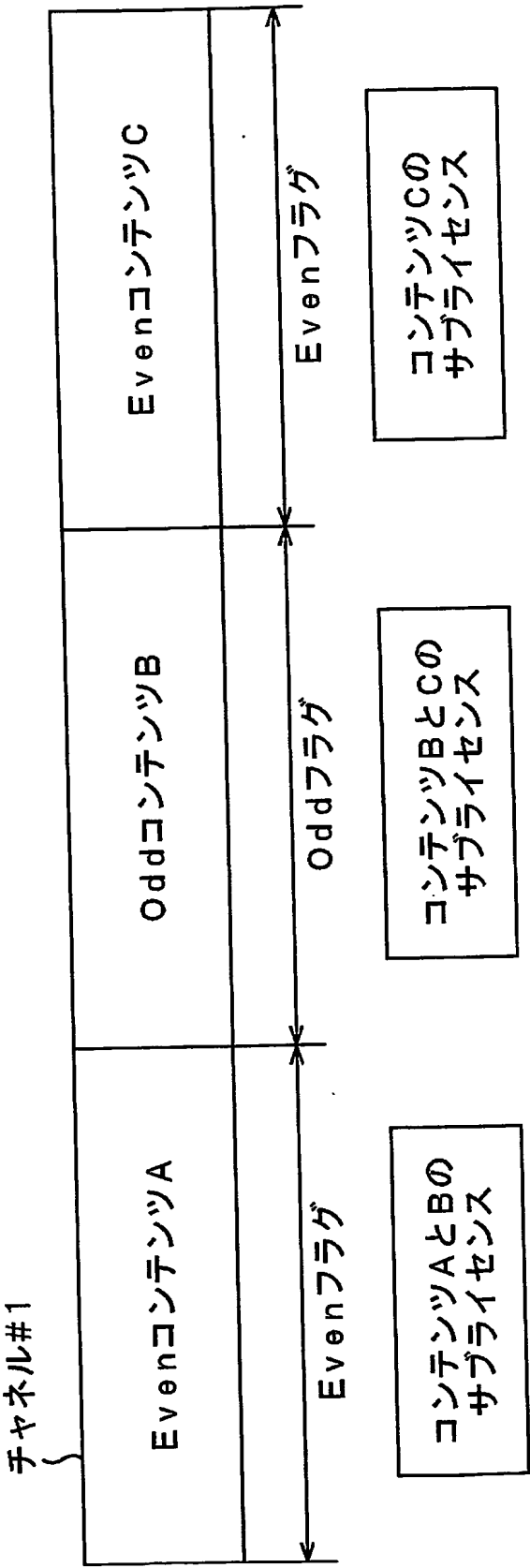


【図 16】

図16

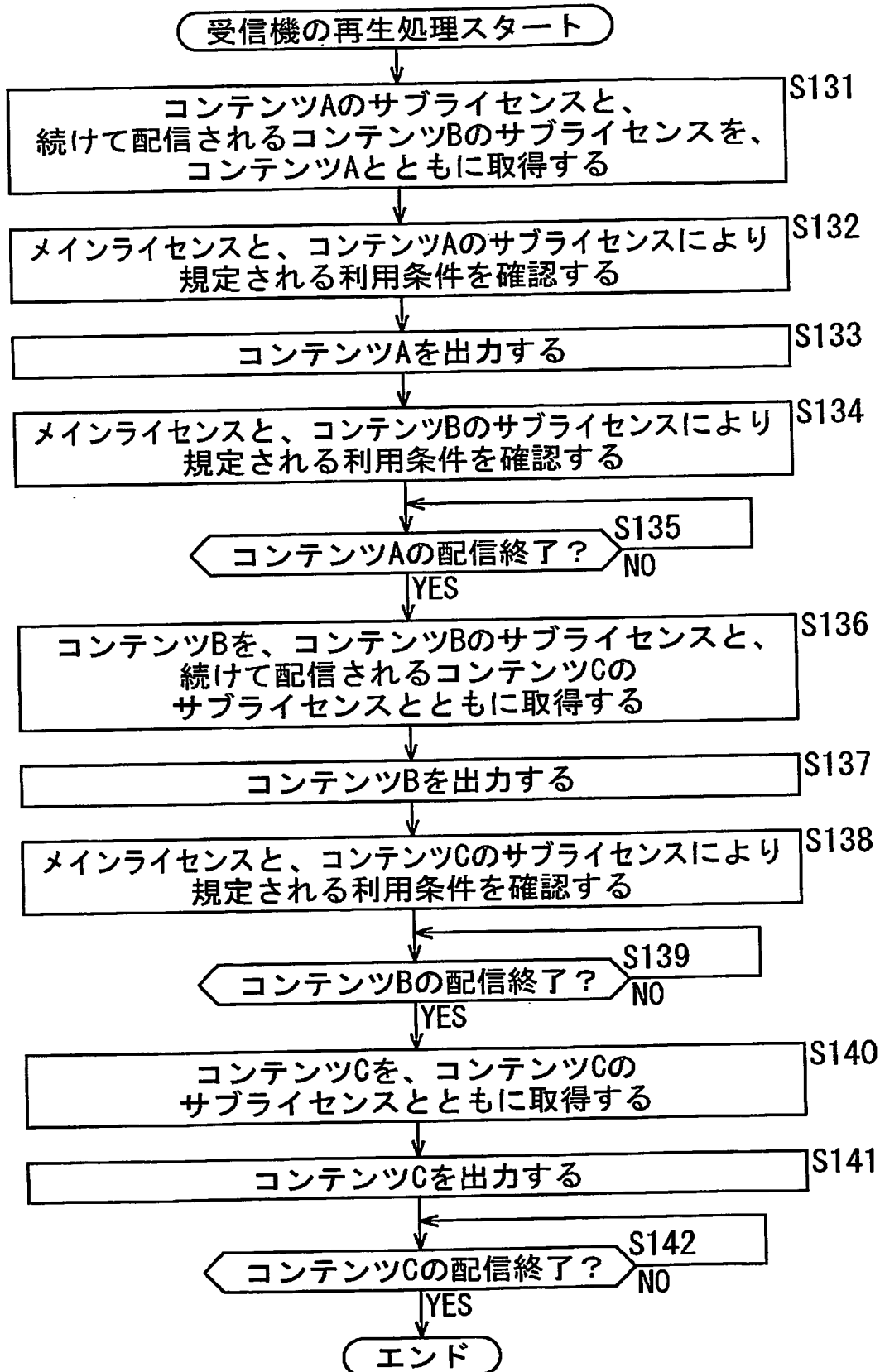


【図 17】
図17

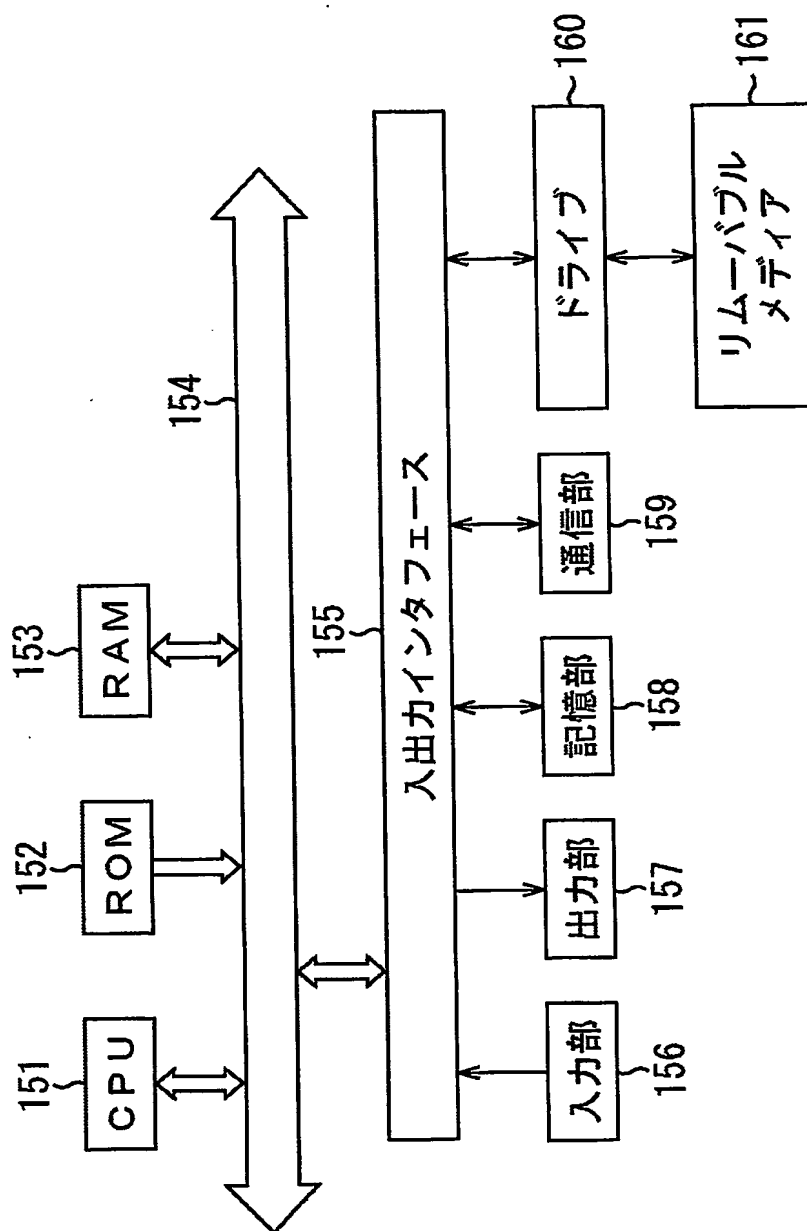


【図 18】

図18



【図 19】
図 19



【書類名】要約書**【要約】**

【課題】 ライセンスを容易に取得できるようにする。また、コンテンツの著作権の保護を図りつつ、様々な形態のサービスに対応できるライセンスを提供することができるようにする。

【解決手段】 コンテンツサーバ12により配信されるコンテンツには、そのコンテンツの利用条件を規定するサブライセンスが付加される。ライセンスサーバ13から、ユーザーが契約するチャンネルで配信されるコンテンツ全体の利用条件を規定するメインライセンスが提供される。コンテンツを再生することが指示されたとき、受信機15-1においては、サブライセンスとメインライセンスで規定される利用条件をともに満たす場合にコンテンツの再生が許可される。本発明は、ネットワークを介して情報を送受信することが可能なパーソナルコンピュータ、コンテンツの取得とその出力を制御するセットトップボックスなどに適用することができる。

【選択図】 図1

特願 2 0 0 3 - 3 8 5 5 9 1

出 願 人 履 歴 情 報

識別番号 [0 0 0 0 0 2 1 8 5]

1. 変更年月日 1 9 9 0 年 8 月 3 0 日

[変更理由] 新規登録

住 所 東京都品川区北品川 6 丁目 7 番 3 5 号

氏 名 ソニー株式会社

特願 2003-385591

出願人履歴情報

識別番号

[000005821]

1. 変更年月日

1990年 8月28日

[変更理由]

新規登録

住 所

大阪府門真市大字門真1006番地

氏 名

松下電器産業株式会社